Códigos electrónicos

Protección de Datos de Carácter Personal

Selección y ordenación:
Santiago Jiménez García, Abogado del Estado.

Edición actualizada a 2 de abril de 2025

BOLETÍN OFICIAL DEL ESTADO

La última versión de este Código en PDF y ePUB está disponible para su descarga **gratuita** en:
www.boe.es/biblioteca_juridica/

Alertas de actualización en Mi BOE: www.boe.es/mi_boe/

Para adquirir el Código en formato papel: tienda.boe.es

Esta obra está sujeta a licencia Creative Commons de Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional, (CC BY-NC-ND 4.0).

© Agencia Estatal Boletín Oficial del Estado
NIPO (PDF): 007-14-179-0
NIPO (Papel): 007-14-205-4
NIPO (ePUB): 007-14-180-3
ISBN: 978-84-340-2157-0
Depósito Legal: M-33794-2014

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

Agencia Estatal Boletín Oficial del Estado
Avenida de Manoteras, 54
28050 MADRID
www.boe.es

SUMARIO

NORMATIVA ESTATAL

§ 1. Constitución Española. [Inclusión parcial] . . . 1

§ 2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales . . . 2

§ 3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. [Inclusión parcial] . . . 64

§ 4. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales . . . 66

§ 5. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal . . . 113

§ 6. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones . . . 166

§ 7. Resolución de 22 de junio de 2001, de la Subsecretaría, por la que se dispone la publicación del Acuerdo de Consejo de Ministros por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información . . . 177

§ 8. Orden de 2 de febrero de 1995 por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos . . . 179

§ 9. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) . . . 181

§ 10. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad . . . 271

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

§ 11. Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos . . . 347

§ 12. Resolución de 24 de mayo de 2010, de la Agencia Española de Protección de Datos, por la que se regula el Registro Electrónico de la Agencia Española de Protección de Datos . . . 372

§ 13. Resolución de 18 de marzo de 2010, de la Agencia Española de Protección de Datos, por la que se crea la Sede Electrónica de la Agencia Española de Protección de Datos . . . 377

SUMARIO

§ 14. Resolución de 1 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos 380

§ 15. Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se crea el Registro Telemático de la Agencia Española de Protección de Datos 383

§ 16. Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático 387

§ 17. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras 393

§ 18. Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones 398

§ 19. Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos 401

§ 20. Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo . . 408

§ 21. Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación 410

§ 22. Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios 414

§ 23. Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal . . 416

§ 24. Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito 418

§ 25. Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General 421

§ 26. Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, de conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de esos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio 428

§ 27. Circular 1/2023, de 26 de junio, sobre la aplicación del artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones 437

NORMATIVA AUTONÓMICA

§ 28. Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos 441

§ 29. Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía 454

§ 30. Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos 484

NORMATIVA ESTATAL SECTORIAL

§ 31. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. [Inclusión parcial] 509

§ 32. Real Decreto-ley 26/2020, de 7 de julio, de medidas de reactivación económica para hacer frente al impacto del COVID-19 en los ámbitos de transportes y vivienda. [Inclusión parcial] 512

§ 33. Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. [Inclusión parcial] 514

§ 34. Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. [Inclusión parcial] 517

§ 35. Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo. [Inclusión parcial] 526

§ 36. Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. [Inclusión parcial] 528

§ 37. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [Inclusión parcial] 530

§ 38. Acuerdo de 23 de julio de 2015, del Pleno del Tribunal Constitucional, por el que se regula la exclusión de los datos de identidad personal en la publicación de las resoluciones jurisdiccionales . 534

§ 39. Ley 23/2015, de 21 de julio, Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social. [Inclusión parcial] 536

§ 40. Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado. [Inclusión parcial] 540

§ 41. Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. [Inclusión parcial] 542

§ 42. Ley 11/2022, de 28 de junio, General de Telecomunicaciones. [Inclusión parcial] 547

§ 43. Ley 5/2014, de 4 de abril, de Seguridad Privada. [Inclusión parcial] 557

§ 44. Ley 26/2013, de 27 de diciembre, de cajas de ahorros y fundaciones bancarias. [Inclusión parcial] . 565

§ 45. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. [Inclusión parcial] 567

§ 46. Ley 4/2013, de 4 de junio, de medidas de flexibilización y fomento del mercado del alquiler de viviendas. [Inclusión parcial] 570

§ 47. Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia. [Inclusión parcial] 572

§ 48. Ley 33/2011, de 4 de octubre, General de Salud Pública. [Inclusión parcial] 574

§ 49. Ley 29/2011, de 22 de septiembre, de Reconocimiento y Protección Integral a las Víctimas del Terrorismo. [Inclusión parcial] 576

§ 50. Ley 26/2011, de 1 de agosto, de adaptación normativa a la Convención Internacional sobre los Derechos de las Personas con Discapacidad. [Inclusión parcial] 577

§ 51. Ley 23/2011, de 29 de julio, de depósito legal. [Inclusión parcial] 578

§ 52. Ley Orgánica 9/2011, de 27 de julio, de derechos y deberes de los miembros de las Fuerzas Armadas. [Inclusión parcial] 580

§ 53. Ley 20/2011, de 21 de julio, del Registro Civil. [Inclusión parcial] 581

§ 54. Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación. [Inclusión parcial] 583

§ 55. Ley 13/2011, de 27 de mayo, de regulación del juego. [Inclusión parcial] 587

§ 56. Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal. [Inclusión parcial] 592

§ 57. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. [Inclusión parcial] 594

§ 58. Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo. [Inclusión parcial] 605

§ 59. Ley 54/2007, de 28 de diciembre, de Adopción internacional. [Inclusión parcial] 610

§ 60. Ley Orgánica 11/2007, de 22 de octubre, reguladora de los derechos y deberes de los miembros de la Guardia Civil. [Inclusión parcial] 611

§ 61. Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. [Inclusión parcial] 612

§ 62. Ley Orgánica 2/2006, de 3 de mayo, de Educación. [Inclusión parcial] 613

§ 63. Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. [Inclusión parcial] 614

§ 64. Ley 58/2003, de 17 de diciembre, General Tributaria. [Inclusión parcial] 615

§ 65. Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas. [Inclusión parcial] 620

§ 66. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica 622

§ 67. Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación. [Inclusión parcial] . . 634

§ 68. Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial] 636

§ 69. Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social. [Inclusión parcial] 638

§ 70. Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. [Inclusión parcial] 641

SUMARIO

§ 71. Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. [Inclusión parcial] 646

§ 72. Ley 14/1986, de 25 de abril, General de Sanidad. [Inclusión parcial] 649

§ 73. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. [Inclusión parcial] 650

§ 74. Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. [Inclusión parcial] 664

§ 75. Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales. [Inclusión parcial] 667

§ 76. Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves 669

§ 77. Real Decreto 957/2020, de 3 de noviembre, por el que se regulan los estudios observacionales con medicamentos de uso humano. [Inclusión parcial] 689

§ 78. Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria. [Inclusión parcial] 691

§ 79. Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia. [Inclusión parcial] 693

§ 80. Ley 10/2021, de 9 de julio, de trabajo a distancia. [Inclusión parcial] 694

§ 81. Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte. [Inclusión parcial] 696

§ 82. Real Decreto 792/2023, de 24 de octubre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte. [Inclusión parcial] 711

§ 83. Ley 19/2021, de 20 de diciembre, por la que se establece el ingreso mínimo vital. [Inclusión parcial] 717

§ 84. Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley Orgánica 8/1980, de 22 de septiembre, de Financiación de las Comunidades Autónomas y otras disposiciones conexas y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial] 719

§ 85. Ley 20/2022, de 19 de octubre, de Memoria Democrática. [Inclusión parcial] 723

§ 86. Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. [Inclusión parcial] 727

§ 87. Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo. [Inclusión parcial] 732

ÍNDICE SISTEMÁTICO

NORMATIVA ESTATAL

§ 1. Constitución Española. [Inclusión parcial] 1

[. . .]

TÍTULO I. De los derechos y deberes fundamentales 1

[. . .]

CAPÍTULO SEGUNDO. Derechos y libertades 1
Sección 1.ª De los derechos fundamentales y de las libertades públicas 1

[. . .]

§ 2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales 2

Preámbulo 2
TÍTULO I. Disposiciones generales 9
TÍTULO II. Principios de protección de datos 10
TÍTULO III. Derechos de las personas 12
CAPÍTULO I. Transparencia e información 12
CAPÍTULO II. Ejercicio de los derechos 13
TÍTULO IV. Disposiciones aplicables a tratamientos concretos 14
TÍTULO V. Responsable y encargado del tratamiento 18
CAPÍTULO I. Disposiciones generales. Medidas de responsabilidad activa 18
CAPÍTULO II. Encargado del tratamiento 20
CAPÍTULO III. Delegado de protección de datos 21
CAPÍTULO IV. Códigos de conducta y certificación 23
TÍTULO VI. Transferencias internacionales de datos 24
TÍTULO VII. Autoridades de protección de datos 25
CAPÍTULO I. La Agencia Española de Protección de Datos 25
Sección 1.ª Disposiciones generales 25
Sección 2.ª Potestades de investigación y planes de auditoría preventiva 29
Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos 31
CAPÍTULO II. Autoridades autonómicas de protección de datos 32
Sección 1.ª Disposiciones generales 32
Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679 33
TÍTULO VIII. Procedimientos en caso de posible vulneración de la normativa de protección de datos 33
TÍTULO IX. Régimen sancionador 37
TÍTULO X. Garantía de los derechos digitales 43
Disposiciones adicionales 49
Disposiciones transitorias 55
Disposiciones derogatorias 56
Disposiciones finales 56

§ 3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. [Inclusión parcial] 64

[. . .]

TÍTULO IV. Disposiciones sectoriales 64

CAPÍTULO I. Ficheros de titularidad pública . . . 64

[. . .]

§ 4. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales . . . 66

Preámbulo . . . 66
CAPÍTULO I. Disposiciones generales . . . 73
CAPÍTULO II. Principios, licitud del tratamiento y videovigilancia . . . 75
Sección 1.ª Principios y licitud del tratamiento . . . 75
Sección 2.ª Tratamiento de datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de Seguridad . . . 79
CAPÍTULO III. Derechos de las personas . . . 81
Sección 1.ª Régimen general . . . 81
Sección 2.ª Régimen especial . . . 84
CAPÍTULO IV. Responsable y encargado de tratamiento . . . 84
Sección 1.ª Obligaciones generales . . . 84
Sección 2.ª Seguridad de los datos personales . . . 88
Sección 3.ª Delegado de protección de datos . . . 90
CAPÍTULO V. Transferencias de datos personales a terceros países que no sean miembros de la Unión Europea o a organizaciones internacionales . . . 91
CAPÍTULO VI. Autoridades de Protección de Datos Independientes . . . 93
CAPÍTULO VII. Reclamaciones . . . 95
CAPÍTULO VIII. Régimen sancionador . . . 97
Disposiciones adicionales . . . 101
Disposiciones transitorias . . . 102
Disposiciones derogatorias . . . 102
Disposiciones finales . . . 102

§ 5. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal . . . 113

Preámbulo . . . 113
Artículos . . . 115
Disposiciones transitorias . . . 115
Disposiciones derogatorias . . . 116
Disposiciones finales . . . 117
REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL . . . 117
TÍTULO I. Disposiciones generales . . . 117
TÍTULO II. Principios de protección de datos . . . 121
CAPÍTULO I. Calidad de los datos . . . 121
CAPÍTULO II. Consentimiento para el tratamiento de los datos y deber de información . . . 123
Sección 1.ª Obtención del consentimiento del afectado . . . 123
Sección 2.ª Deber de información al interesado . . . 125
CAPÍTULO III. Encargado del tratamiento . . . 125
TÍTULO III. Derechos de acceso, rectificación, cancelación y oposición . . . 126
CAPÍTULO I. Disposiciones generales . . . 126
CAPÍTULO II. Derecho de acceso . . . 128
CAPÍTULO III. Derechos de rectificación y cancelación . . . 130
CAPÍTULO IV. Derecho de oposición . . . 130
TÍTULO IV. Disposiciones aplicables a determinados ficheros de titularidad privada . . . 131
CAPÍTULO I. Ficheros de información sobre solvencia patrimonial y crédito . . . 131
Sección 1.ª Disposiciones generales . . . 131
Sección 2.ª Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés . . . 132
CAPÍTULO II. Tratamientos para actividades de publicidad y prospección comercial . . . 134
TÍTULO V. Obligaciones previas al tratamiento de los datos . . . 137
CAPÍTULO I. Creación, modificación o supresión de ficheros de titularidad pública . . . 137
CAPÍTULO II. Notificación e inscripción de los ficheros de titularidad pública o privada . . . 138
TÍTULO VI. Transferencias internacionales de datos . . . 141
CAPÍTULO I. Disposiciones generales . . . 141

CAPÍTULO II. Transferencias a estados que proporcionen un nivel adecuado de protección . . . 141
CAPÍTULO III. Transferencias a Estados que no proporcionen un nivel adecuado de protección . . . 142
TÍTULO VII. Códigos tipo . . . 143
TÍTULO VIII. De las medidas de seguridad en el tratamiento de datos de carácter personal . . . 146
CAPÍTULO I. Disposiciones generales . . . 146
CAPÍTULO II. Del documento de seguridad . . . 148
CAPÍTULO III. Medidas de seguridad aplicables a ficheros y tratamientos automatizados . . . 149
Sección 1.ª Medidas de seguridad de nivel básico . . . 149
Sección 2.ª Medidas de seguridad de nivel medio . . . 151
Sección 3.ª Medidas de seguridad de nivel alto . . . 152
CAPÍTULO IV. Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados . . . 153
Sección 1.ª Medidas de seguridad de nivel básico . . . 153
Sección 2.ª Medidas de seguridad de nivel medio . . . 154
Sección 3.ª Medidas de seguridad de nivel alto . . . 154
TÍTULO IX. Procedimientos tramitados por la Agencia Española de Protección de Datos . . . 155
CAPÍTULO I. Disposiciones generales . . . 155
CAPÍTULO II. Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición . . . 155
CAPÍTULO III. Procedimientos relativos al ejercicio de la potestad sancionadora . . . 156
Sección 1.ª Disposiciones generales . . . 156
Sección 2.ª Actuaciones previas . . . 157
Sección 3.ª Procedimiento sancionador . . . 158
Sección 4.ª Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las administraciones públicas . . . 158
CAPÍTULO IV. Procedimientos relacionados con la inscripción o cancelación de ficheros . . . 159
Sección 1.ª Procedimiento de inscripción de la creación, modificación o supresión de ficheros . . . 159
Sección 2.ª Procedimiento de cancelación de oficio de ficheros inscritos . . . 160
CAPÍTULO V. Procedimientos relacionados con las transferencias internacionales de datos . . . 160
Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos . . . 160
Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos . . . 161
CAPÍTULO VI. Procedimiento de inscripción de códigos tipo . . . 162
CAPÍTULO VII. Otros procedimientos tramitados por la agencia española de protección de datos . . . 163
Sección 1.ª Procedimiento de exención del deber de información al interesado . . . 163
Sección 2.ª Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos . . . 164
Disposiciones adicionales . . . 165

§ 6. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones . . . 166

Preámbulo . . . 166
CAPÍTULO I. Disposiciones generales . . . 168
CAPÍTULO II. Conservación y cesión de datos . . . 170
CAPÍTULO III. Infracciones y sanciones . . . 172
Disposiciones adicionales . . . 172
Disposiciones transitorias . . . 173
Disposiciones derogatorias . . . 173
Disposiciones finales . . . 174

§ 7. Resolución de 22 de junio de 2001, de la Subsecretaría, por la que se dispone la publicación del Acuerdo de Consejo de Ministros por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información . . . 177

Parte dispositiva . . . 177
ANEXO. Acuerdo por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información . . . 177

§ 8. Orden de 2 de febrero de 1995 por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos . . . 179

Preámbulo . . . 179
Artículos . . . 179
Disposiciones finales . . . 180

§ 9. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) 181

Preámbulo 181
CAPÍTULO I. Disposiciones generales 216
CAPÍTULO II. Principios 220
CAPÍTULO III. Derechos del interesado 224
Sección 1. Transparencia y modalidades 224
Sección 2. Información y acceso a los datos personales 225
Sección 3. Rectificación y supresión 227
Sección 4. Derecho de oposición y decisiones individuales automatizadas 229
Sección 5. Limitaciones 230
CAPÍTULO IV. Responsable del tratamiento y encargado del tratamiento 231
Sección 1. Obligaciones generales 231
Sección 2. Seguridad de los datos personales 235
Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa 236
Sección 4. Delegado de protección de datos 238
Sección 5. Códigos de conducta y certificación 240
CAPÍTULO V. Transferencias de datos personales a terceros países u organizaciones internacionales 244
CAPÍTULO VI. Autoridades de control independientes 249
Sección 1. Independencia 249
Sección 2. Competencia, funciones y poderes 250
CAPÍTULO VII. Cooperación y coherencia 254
Sección 1. Cooperación y coherencia 254
Sección 2. Coherencia 257
Sección 3. Comité europeo de protección de datos 259
CAPÍTULO VIII. Recursos, responsabilidad y sanciones 263
CAPÍTULO IX. Disposiciones relativas a situaciones específicas de tratamiento 266
CAPÍTULO X. Actos delegados y actos de ejecución 268
CAPÍTULO XI. Disposiciones finales 269

§ 10. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad 271

Preámbulo 271
CAPÍTULO I. Disposiciones generales 278
CAPÍTULO II. Principios básicos 279
CAPÍTULO III. Política de seguridad y requisitos mínimos de seguridad 281
CAPÍTULO IV. Seguridad de los sistemas: auditoría, informe e incidentes de seguridad 287
CAPÍTULO V. Normas de conformidad 289
CAPÍTULO VI. Actualización del Esquema Nacional de Seguridad 290
CAPÍTULO VII. Categorización de los sistemas de información 290
Disposiciones adicionales 291
Disposiciones transitorias 291
Disposiciones derogatorias 291
Disposiciones finales 292
ANEXO I. Categorías de seguridad de los sistemas de información 292
ANEXO II. Medidas de Seguridad 294
ANEXO III. Auditoría de la seguridad 342
ANEXO IV. Glosario 343

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

§ 11. Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos 347

Preámbulo 347
Artículos 350
Disposiciones adicionales 350
Disposiciones transitorias 350

Disposiciones derogatorias . . . 350
Disposiciones finales . . . 350
ESTATUTO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS . . . 351
CAPÍTULO I. Disposiciones generales . . . 351
CAPÍTULO II. Estructura orgánica de la Agencia Española de Protección de Datos . . . 354
Sección 1.ª De la Presidencia de la Agencia Española de Protección de Datos . . . 354
Sección 2.ª La Adjuntía a la Presidencia de la Agencia Española de Protección de Datos . . . 356
Sección 3.ª Procedimiento de designación de la Presidencia y la Adjuntía . . . 357
Sección 4.ª El Consejo Consultivo de la Agencia Española de Protección de Datos . . . 359
Sección 5.ª Otros órganos directamente dependientes de la Presidencia de la Agencia Española de Protección de Datos . . . 360
CAPÍTULO III. Personal al servicio de la Agencia Española de Protección de Datos . . . 366
CAPÍTULO IV. Régimen económico, presupuestario, patrimonial y de contratación . . . 368
Sección 1.ª Régimen económico-financiero, patrimonial y de contratación . . . 368
Sección 2.ª Régimen presupuestario, de contabilidad y control económico-financiero . . . 369
CAPÍTULO V. Asesoramiento jurídico de la Agencia Española de Protección de Datos . . . 371

§ 12. Resolución de 24 de mayo de 2010, de la Agencia Española de Protección de Datos, por la que se regula el Registro Electrónico de la Agencia Española de Protección de Datos . . . 372

Preámbulo . . . 372
Artículos . . . 373
Disposiciones transitorias . . . 376
Disposiciones derogatorias . . . 376
Disposiciones finales . . . 376
ANEXO I. Procedimientos competencia de la Agencia Española de Protección de Datos admisibles a través de su Registro Electrónico . . . 376

§ 13. Resolución de 18 de marzo de 2010, de la Agencia Española de Protección de Datos, por la que se crea la Sede Electrónica de la Agencia Española de Protección de Datos . . . 377

Preámbulo . . . 377
Artículos . . . 378
Disposiciones finales . . . 379

§ 14. Resolución de 1 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos . . . 380

Preámbulo . . . 380
Artículos . . . 381

§ 15. Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se crea el Registro Telemático de la Agencia Española de Protección de Datos . . . 383

Preámbulo . . . 383
Artículos . . . 384

§ 16. Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático . . . 387

Preámbulo . . . 387
Artículos . . . 390
ANEXOS . . . 392

§ 17. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras . . . 393

Preámbulo . . . 393
Artículos . . . 395

Disposiciones transitorias . . . 396
Disposiciones finales . . . 396
ANEXO. 1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. . . . 396

§ 18. Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones . . . 398

Preámbulo . . . 398
Artículos . . . 399

§ 19. Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos . . . 401

Preámbulo . . . 401
Sección I. Disposiciones generales . . . 403
Sección II. Disposiciones aplicables a transferencias concretas . . . 404

§ 20. Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo . . . 408

Preámbulo . . . 408
Artículos . . . 408

§ 21. Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación . . . 410

Preámbulo . . . 410
Artículos . . . 410
Disposiciones finales . . . 413

§ 22. Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios . . . 414

Preámbulo . . . 414
Artículos . . . 414

§ 23. Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal . . . 416

Preámbulo . . . 416
Artículos . . . 416

§ 24. Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito . . . 418

Preámbulo . . . 418
CAPÍTULO I. Calidad de los datos objeto del tratamiento automatizado, forma y veces en que debe efectuarse la notificación y cómputo del plazo al que se refiere el artículo 28.3 de la Ley Orgánica . . . 419
CAPITULO II. Medidas de seguridad . . . 420

§ 25. Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, 421

federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General . . . . . .

Preámbulo 421
Artículos 423
Disposiciones transitorias 427
Disposiciones finales 427

§ 26. Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, de conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de esos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio 428

Preámbulo 428
Artículos 431
CAPÍTULO I. Función consultiva dirigida al Parlamento, al Gobierno y a las Administraciones Públicas relativa al desarrollo y aplicación de las normas que incidan en materia propia del RGPD y la LOPDPGDD [artículo 57.1.e) RGPD] 431
CAPÍTULO II. Función consultiva dirigida a los ciudadanos para facilitar información sobre el ejercicio de sus derechos [artículo 57.1.e) RGPD] 432
CAPÍTULO III. Función consultiva dirigida a los Delegados de Protección de Datos (DPD) conforme al artículo 39.1.e) del RGPD 433
CAPÍTULO IV. Función consultiva sobre las operaciones de tratamiento contempladas en el artículo 36.2 del RGPD [artículo 57.1.l) RGPD] 434
CAPÍTULO V. Actividades de información y sensibilización 435
Disposiciones adicionales 436
Disposiciones finales 436

§ 27. Circular 1/2023, de 26 de junio, sobre la aplicación del artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones 437

Preámbulo 437
Artículos 439
Disposiciones finales 440

NORMATIVA AUTONÓMICA

§ 28. Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos 441

Preámbulo 441
CAPÍTULO I. Disposiciones generales 442
CAPÍTULO II. Organización 444
CAPÍTULO III. Relaciones con otros organismos e instituciones 447
CAPÍTULO IV. Ejercicio de competencias y funciones 448
CAPÍTULO V. Régimen jurídico, de personal, económico y de contratación 451
Disposiciones transitorias 452
Disposiciones derogatorias 453
Disposiciones finales 453

§ 29. Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía 454

Preámbulo 454
TÍTULO I. Disposiciones generales 460
TÍTULO II. La publicidad activa 465
TÍTULO III. El derecho de acceso a la información pública 470
CAPÍTULO I. Normas generales 470
CAPÍTULO II. El ejercicio del derecho de acceso a la información pública 471
TÍTULO IV. Fomento de la transparencia 472

TÍTULO V. Organización . . . 473
CAPÍTULO I. Coordinación y planificación en el ámbito de la Junta de Andalucía . . . 473
CAPÍTULO II. Consejo de Transparencia y Protección de Datos de Andalucía . . . 474
TÍTULO VI. Régimen sancionador . . . 476
Disposiciones adicionales . . . 479
Disposiciones transitorias . . . 480
Disposiciones derogatorias . . . 480
Disposiciones finales . . . 480

§ 30. Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos . . . 484

Preámbulo . . . 484
CAPÍTULO I. Disposiciones generales . . . 491
CAPÍTULO II. La Autoridad Vasca de Protección de Datos . . . 492
Sección 1.ª Organización y régimen jurídico . . . 492
Sección 2.ª Órganos de la Autoridad Vasca de Protección de Datos . . . 494
Sección 3.ª Potestad de investigación . . . 496
Sección 4.ª Potestad normativa . . . 497
Sección 5.ª Otras competencias de la Autoridad Vasca de Protección de Datos . . . 497
Sección 6.ª Cooperación con otras autoridades de protección de datos . . . 499
CAPÍTULO III. Régimen sancionador. Potestad correctiva de la Autoridad Vasca de Protección de Datos . . . 500
CAPÍTULO IV. Procedimientos en caso de infracción de las normas de protección de datos . . . 502
Sección 1.ª Disposiciones generales . . . 502
Sección 2.ª Iniciación del procedimiento . . . 503
Sección 3.ª Procedimiento en caso de reclamaciones derivadas del ejercicio de derechos . . . 505
Sección 4.ª Procedimiento de ejercicio de la potestad sancionadora . . . 505
Sección 5.ª Especialidades en caso de procedimientos referidos a tratamientos transfronterizos . . . 506
Disposiciones adicionales . . . 507
Disposiciones transitorias . . . 508
Disposiciones derogatorias . . . 508
Disposiciones finales . . . 508

NORMATIVA ESTATAL SECTORIAL

§ 31. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. [Inclusión parcial] . . . 509

[. . .]

TÍTULO III. Obligaciones y responsabilidad de los prestadores de servicios electrónicos de confianza . . . 509

[. . .]

§ 32. Real Decreto-ley 26/2020, de 7 de julio, de medidas de reactivación económica para hacer frente al impacto del COVID-19 en los ámbitos de transportes y vivienda. [Inclusión parcial] . 512

[. . .]

CAPÍTULO II. Medidas en el sector del transporte aéreo . . . 512

[. . .]

Disposiciones adicionales . . . 513

§ 33. Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. [Inclusión parcial] . . . 514

[. . .]

TÍTULO III. Derechos y obligaciones en relación con la prestación y utilización de servicios de pago . . . 514

[. . .]

CAPÍTULO II. Autorización de operaciones de pago . . . 514

[. . .]

CAPÍTULO IV. Protección de datos . . . 516

[. . .]

§ 34. Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. [Inclusión parcial] . . . 517

[. . .]

LIBRO PRIMERO. Configuración general de la contratación del sector público y elementos estructurales de los contratos . . . 517
TÍTULO I. Disposiciones generales sobre la contratación del sector público . . . 517

[. . .]

CAPÍTULO II. Libertad de pactos y contenido mínimo del contrato . . . 517

[. . .]

LIBRO SEGUNDO. De los contratos de las Administraciones Públicas . . . 518
TÍTULO I. Disposiciones generales . . . 518
CAPÍTULO I. De las actuaciones relativas a la contratación de las Administraciones Públicas . . . 518

[. . .]

Subsección 2.ª Pliegos de cláusulas administrativas y de prescripciones técnicas . . . 518
Sección 2.ª De la adjudicación de los contratos de las Administraciones Públicas . . . 520
Subsección 1.ª Normas generales . . . 520

[. . .]

Sección 3.ª De los efectos, cumplimiento y extinción de los contratos administrativos . . . 520

[. . .]

Subsección 3.ª Ejecución de los contratos . . . 520

[. . .]

Subsección 5.ª Suspensión y extinción de los contratos . . . 522

[. . .]

LIBRO CUARTO. Organización administrativa para la gestión de la contratación . . . 523

[. . .]

TÍTULO II. Registros Oficiales . . . 524

[. . .]

CAPÍTULO II. Registro de Contratos del Sector Público . . . 524

[. . .]

Disposiciones adicionales . . . 525

§ 35. Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo. [Inclusión parcial] . . . 526

[. . .]

TÍTULO II. Obligaciones de las entidades de resolución alternativa acreditadas . . . 526

[. . .]

§ 36. Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. [Inclusión parcial] 528

TÍTULO I. De la relación individual de trabajo 528
CAPÍTULO I. Disposiciones generales 528

[. . .]

[. . .]

CAPÍTULO II. Contenido del contrato de trabajo 529

[. . .]

§ 37. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [Inclusión parcial]. . . . 530

TÍTULO PRELIMINAR. Disposiciones generales, principios de actuación y funcionamiento del sector público 530
CAPÍTULO I. Disposiciones generales 530

[. . .]

CAPÍTULO V. Funcionamiento electrónico del sector público 531

[. . .]

§ 38. Acuerdo de 23 de julio de 2015, del Pleno del Tribunal Constitucional, por el que se regula la exclusión de los datos de identidad personal en la publicación de las resoluciones jurisdiccionales 534

Preámbulo 534
Artículos 534
Disposiciones transitorias 534
Disposiciones finales 535

§ 39. Ley 23/2015, de 21 de julio, Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social. [Inclusión parcial]. 536

[. . .]

TÍTULO II. Funcionamiento del Sistema 536
CAPÍTULO I. De las funciones de la Inspección de Trabajo y Seguridad Social. 536
CAPÍTULO II. De las actuaciones de la Inspección de Trabajo y Seguridad Social. 538

[. . .]

Disposiciones adicionales 539

§ 40. Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado. [Inclusión parcial] 540

[. . .]

TÍTULO III. Órganos de vigilancia y control de los altos cargos de la Administración General del Estado 540

[. . .]

§ 41. Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. [Inclusión parcial] 542

TÍTULO I. De las entidades de crédito 542
CAPÍTULO I. Disposiciones generales 542

[. . .]

TÍTULO III. Supervisión. 544
CAPÍTULO I. Función supervisora 544

[...]

CAPÍTULO VI. Obligaciones de información y publicación . . . 545

[...]

§ 42. Ley 11/2022, de 28 de junio, General de Telecomunicaciones. [Inclusión parcial] . . . 547

[...]

TÍTULO III. Obligaciones de servicio público y derechos y obligaciones de carácter público en el suministro de redes y en la prestación de servicios de comunicaciones electrónicas . . . 547

[...]

CAPÍTULO II. Derechos de los operadores y despliegue de redes públicas de comunicaciones electrónicas . . . 547
Sección 1.ª Derechos de los operadores a la ocupación del dominio público, a ser beneficiarios en el procedimiento de expropiación forzosa y al establecimiento a su favor de servidumbres y de limitaciones a la propiedad . . . 547

[...]

CAPÍTULO III. Salvaguardia de derechos fundamentales, secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas . . . 550

[...]

§ 43. Ley 5/2014, de 4 de abril, de Seguridad Privada. [Inclusión parcial] . . . 557

[...]

TÍTULO I. Coordinación . . . 557

[...]

TÍTULO IV. Servicios y medidas de seguridad . . . 557

[...]

CAPÍTULO II. Servicios de las empresas de seguridad privada . . . 558
CAPÍTULO III. Servicios de los despachos de detectives privados . . . 558

[...]

TÍTULO VI. Régimen sancionador . . . 560
CAPÍTULO I. Infracciones . . . 560

[...]

§ 44. Ley 26/2013, de 27 de diciembre, de cajas de ahorros y fundaciones bancarias. [Inclusión parcial] . . . 565

[...]

TÍTULO II. De las fundaciones bancarias . . . 565

[...]

CAPÍTULO V. Régimen de control . . . 565

[...]

§ 45. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. [Inclusión parcial] . . . 567

[...]

TÍTULO I. Transparencia de la actividad pública . . . 567

[. . .]

CAPÍTULO II. Publicidad activa . . . 567
CAPÍTULO III. Derecho de acceso a la información pública . . . 568

[. . .]

TÍTULO III. Consejo de Transparencia y Buen Gobierno . . . 569
Disposiciones adicionales . . . 569

§ 46. Ley 4/2013, de 4 de junio, de medidas de flexibilización y fomento del mercado del alquiler de viviendas. [Inclusión parcial]. . . . 570

Artículos . . . 570
Disposiciones adicionales . . . 571

§ 47. Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia. [Inclusión parcial] . . . 572

[. . .]

CAPÍTULO II. Funciones . . . 572

[. . .]

§ 48. Ley 33/2011, de 4 de octubre, General de Salud Pública. [Inclusión parcial] . . . 574

[. . .]

TÍTULO I. Derechos, deberes y obligaciones en salud pública . . . 574
CAPÍTULO I. Derechos de los ciudadanos . . . 574

[. . .]

CAPÍTULO IX. Sistema de Información en Salud Pública. . . . 574

[. . .]

§ 49. Ley 29/2011, de 22 de septiembre, de Reconocimiento y Protección Integral a las Víctimas del Terrorismo. [Inclusión parcial] . . . 576

[. . .]

TÍTULO CUARTO. Régimen de protección social . . . 576

[. . .]

[. . .]

§ 50. Ley 26/2011, de 1 de agosto, de adaptación normativa a la Convención Internacional sobre los Derechos de las Personas con Discapacidad. [Inclusión parcial] . . . 577

Disposiciones adicionales . . . 577

§ 51. Ley 23/2011, de 29 de julio, de depósito legal. [Inclusión parcial] . . . 578

CAPÍTULO I. Disposiciones generales . . . 578
CAPÍTULO II. De la obligación del depósito legal . . . 578

[. . .]

§ 52. Ley Orgánica 9/2011, de 27 de julio, de derechos y deberes de los miembros de las Fuerzas Armadas. [Inclusión parcial] 580

[. . .]

TÍTULO I. Del ejercicio de los derechos fundamentales y libertades públicas 580

[. . .]

§ 53. Ley 20/2011, de 21 de julio, del Registro Civil. [Inclusión parcial] 581

TÍTULO I. El Registro Civil. Disposiciones generales 581
CAPÍTULO PRIMERO. Naturaleza, contenido y competencias del Registro Civil 581

[. . .]

Disposiciones adicionales 581
Disposiciones finales 582

§ 54. Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación. [Inclusión parcial] . . . 583

[. . .]

TÍTULO II. Recursos humanos dedicados a la investigación 583
CAPÍTULO I. Personal Investigador al servicio de las Universidades públicas, de los Organismos Públicos de Investigación y de los Organismos de investigación de otras Administraciones Públicas 583

[. . .]

[. . .]

CAPÍTULO II. Especificidades aplicables al personal al servicio de los Organismos Públicos de Investigación de la Administración General del Estado 584

[. . .]

Sección 2.ª Personal de investigación al servicio de los organismos públicos de Investigación de la Administración General del Estado 584

[. . .]

§ 55. Ley 13/2011, de 27 de mayo, de regulación del juego. [Inclusión parcial] 587

[. . .]

TÍTULO IV. Control de la actividad 587

[. . .]

CAPÍTULO II. Participantes 587
CAPÍTULO III. Homologación de los sistemas técnicos de juego 588
TÍTULO V. La Administración del Juego 589

[. . .]

§ 56. Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal. [Inclusión parcial]. 592

[. . .]

TÍTULO II. Derechos de los usuarios de los servicios postales 592

[. . .]

TÍTULO V. Acceso a la red postal de los operadores y resolución de conflictos entre ellos 592
CAPÍTULO I. Acceso a la red postal y a otras infraestructuras postales. 592

[. . .]

Disposiciones finales . . . 593

§ 57. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. [Inclusión parcial] . . . 594

[. . .]

CAPÍTULO II. De la diligencia debida . . . 594

[. . .]

Sección 3.ª Medidas reforzadas de diligencia debida . . . 594
CAPÍTULO III. De las obligaciones de información . . . 595
CAPÍTULO IV. Del control interno . . . 596

[. . .]

CAPÍTULO VI. Otras disposiciones . . . 600

[. . .]

§ 58. Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo. [Inclusión parcial] . . . 605

[. . .]

TÍTULO I. Responsabilidad institucional en el ámbito de la salud, los derechos sexuales y reproductivos . . . 605

[. . .]

CAPÍTULO IV. Medidas para la aplicación efectiva de la ley . . . 605
TÍTULO II. De la interrupción voluntaria del embarazo . . . 606

[. . .]

CAPÍTULO II. Garantías en el acceso a la prestación . . . 606

[. . .]

Disposiciones adicionales . . . 608

§ 59. Ley 54/2007, de 28 de diciembre, de Adopción internacional. [Inclusión parcial] . . . 610

TÍTULO I. Disposiciones generales . . . 610

[. . .]

CAPÍTULO III. Capacidad y requisitos para la adopción internacional . . . 610

[. . .]

§ 60. Ley Orgánica 11/2007, de 22 de octubre, reguladora de los derechos y deberes de los miembros de la Guardia Civil. [Inclusión parcial]. . . . 611

[. . .]

TÍTULO II. Del ejercicio de derechos fundamentales y libertades públicas . . . 611

[. . .]

§ 61. Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. [Inclusión parcial] 612

§ 62. Ley Orgánica 2/2006, de 3 de mayo, de Educación. [Inclusión parcial] 613

[. . .]

Disposiciones adicionales 613

§ 63. Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. [Inclusión parcial]. 614

[. . .]

TÍTULO V. Tutela Judicial 614

[. . .]

CAPÍTULO IV. Medidas judiciales de protección y de seguridad de las víctimas 614

[. . .]

§ 64. Ley 58/2003, de 17 de diciembre, General Tributaria. [Inclusión parcial] 615

[. . .]

TÍTULO III. La aplicación de los tributos 615
CAPÍTULO I. Principios generales 615

[. . .]

Sección 3.ª Colaboración social en la aplicación de los tributos 615

[. . .]

§ 65. Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas. [Inclusión parcial] 620

[. . .]

TÍTULO V. Gestión patrimonial 620

[. . .]

CAPÍTULO V. Enajenación y gravamen 620

[. . .]

Sección 2.ª Enajenación de inmuebles 620

[. . .]

§ 66. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica 622

Preámbulo 622
CAPÍTULO I. Principios generales 624
CAPÍTULO II. El derecho de información sanitaria 625
CAPÍTULO III. Derecho a la intimidad 626
CAPÍTULO IV. El respeto de la autonomía del paciente 626
CAPÍTULO V. La historia clínica 629
CAPÍTULO VI. Informe de alta y otra documentación clínica 632
Disposiciones adicionales 632
Disposiciones transitorias 633
Disposiciones derogatorias 633

Disposiciones finales . . . 633

§ 67. Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación. [Inclusión parcial] . . . 634

[. . .]

CAPÍTULO III. Funcionamiento de las asociaciones . . . 634

[. . .]

CAPÍTULO V. Registros de Asociaciones . . . 634

[. . .]

§ 68. Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial] . . . 636

[. . .]

TÍTULO VII. De la ejecución de las medidas . . . 636

[. . .]

CAPÍTULO II. Reglas para la ejecución de las medidas . . . 636

[. . .]

Disposiciones adicionales . . . 637

§ 69. Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social. [Inclusión parcial] . . . 638

[. . .]

TÍTULO II. Régimen jurídico de los extranjeros . . . 638
CAPÍTULO I. De la entrada y salida del territorio español . . . 638

[. . .]

Disposiciones adicionales . . . 639

§ 70. Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. [Inclusión parcial] . . . 641

TÍTULO I. Del orden jurisdiccional contencioso-administrativo . . . 641

[. . .]

CAPÍTULO II. Órganos y competencias . . . 641

[. . .]

TÍTULO V. Procedimientos especiales . . . 644
CAPÍTULO I. Procedimiento para la protección de los derechos fundamentales de la persona . . . 644

[. . .]

§ 71. Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. [Inclusión parcial] . . . 646

Artículos . . . 646
Disposiciones adicionales . . . 647

§ 72. Ley 14/1986, de 25 de abril, General de Sanidad. [Inclusión parcial] . . . 649

[. . .]

TÍTULO VI. De la docencia y la investigación . . . 649

[. . .]

CAPÍTULO II. Tratamiento de datos de la investigación en salud 649

[. . .]

§ 73. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. [Inclusión parcial] 650

[. . .]

TÍTULO IV. De la composición y atribuciones de los órganos jurisdiccionales 650
CAPÍTULO I. Del Tribunal Supremo 650
CAPÍTULO II. De la Audiencia Nacional 651
CAPÍTULO III. De los Tribunales Superiores de Justicia 651

[. . .]

CAPÍTULO V. De los Tribunales de Instancia y del Tribunal Central de Instancia 652

[. . .]

TÍTULO III. De las actuaciones judiciales 653
CAPÍTULO I. De la oralidad, publicidad y lengua oficial 653
CAPÍTULO I BIS. Protección de datos de carácter personal en el ámbito de la Administración de Justicia . . . 653

[. . .]

CAPÍTULO II. De la oficina judicial 658
CAPÍTULO III. De las unidades administrativas 658
CAPÍTULO IV. De las Oficinas de Justicia en los municipios 658
CAPÍTULO V. De la oficina fiscal 660

[. . .]

LIBRO VIII. Del Consejo General del Poder Judicial 660
TÍTULO I. De las atribuciones del Consejo General del Poder Judicial 660

[. . .]

CAPÍTULO VIII. La Comisión de Supervisión y Control de Protección de Datos 662

[. . .]

Sección 7.ª La Dirección de Supervisión y Control de Protección de Datos 663

[. . .]

§ 74. Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. [Inclusión parcial] 664

[. . .]

TÍTULO PRIMERO. Disposiciones comunes para las elecciones por sufragio universal directo 664

[. . .]

CAPÍTULO IV. El censo electoral 664

[. . .]

Sección III. Rectificación del censo en período electoral 664
Sección IV. Acceso a los datos censales 665

[. . .]

CAPÍTULO VI. Procedimiento electoral 665

[. . .]

Sección V. Propaganda y actos de campaña electoral 666

[. . .]

§ 75. Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales. [Inclusión parcial] 667

[. . .]

LIBRO SEGUNDO. Medidas para la adaptación del derecho español a la normativa de la Unión Europea en materia de seguros privados y planes y fondos de pensiones 667
TÍTULO I. Transposición de la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros 667

[. . .]

CAPÍTULO III. De las actividades de los distribuidores de seguros y de reaseguros residentes o domiciliados en España 667

[. . .]

Sección 7.ª Competencias de ordenación y supervisión 667

[. . .]

Subsección 3.ª Protección de datos de carácter personal 667

[. . .]

§ 76. Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves 669

Preámbulo 669
CAPÍTULO I. Disposiciones generales 674
CAPÍTULO II. Tratamiento de los datos PNR 676
CAPÍTULO III. Régimen sancionador 684
Sección 1.ª Disposiciones generales 684
Sección 2.ª Infracciones 685
Sección 3.ª Sanciones 685
Sección 4.ª Normas especiales de procedimiento sancionador 686
Disposiciones adicionales 686
Disposiciones finales 687

§ 77. Real Decreto 957/2020, de 3 de noviembre, por el que se regulan los estudios observacionales con medicamentos de uso humano. [Inclusión parcial] 689

[. . .]

CAPÍTULO II. Condiciones para la realización de los estudios observacionales con medicamentos 689

[. . .]

§ 78. Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria. [Inclusión parcial]. 691

[. . .]

TÍTULO II. Del régimen penitenciario 691
CAPÍTULO I. Organización general 691

[. . .]

§ 79. Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia. [Inclusión parcial] 693

[. . .]

CAPÍTULO XII. De la Agencia Española de Protección de Datos . . . 693

[. . .]

§ 80. Ley 10/2021, de 9 de julio, de trabajo a distancia. [Inclusión parcial] . . . 694

[. . .]

CAPÍTULO III. Derechos de las personas trabajadoras a distancia . . . 694

[. . .]

Sección 5.ª Derechos relacionados con el uso de medios digitales . . . 694

[. . .]

CAPÍTULO IV. Facultades de organización, dirección y control empresarial en el trabajo a distancia . . . 695

§ 81. Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte. [Inclusión parcial] . . . 696

TÍTULO PRELIMINAR. Disposiciones generales . . . 696

[. . .]

CAPÍTULO II. Organización administrativa para la lucha contra el dopaje . . . 696
TÍTULO I. Controles de dopaje . . . 697
TÍTULO II. Régimen sancionador en materia de dopaje . . . 699

[. . .]

CAPÍTULO II. Del procedimiento para la imposición de sanciones . . . 699

[. . .]

TÍTULO III. Tratamiento de datos personales relativos al dopaje . . . 700
TÍTULO IV. Control y supervisión general de los productos susceptibles de producir dopaje en el deporte . . . 701
CAPÍTULO I. Medidas de control y supervisión de productos, medicamentos y complementos nutricionales . . . 701

[. . .]

Disposiciones adicionales . . . 702
ANEXO. Definiciones . . . 704

§ 82. Real Decreto 792/2023, de 24 de octubre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte. [Inclusión parcial] . . . 711

TÍTULO PRELIMINAR. Disposiciones generales . . . 711
TÍTULO I. Autorizaciones de uso terapéutico . . . 711

[. . .]

TÍTULO III. Control del dopaje . . . 712
CAPÍTULO I. Planificación de controles . . . 712

[. . .]

CAPÍTULO III. Realización de controles . . . 713
Sección 1.ª Disposiciones generales . . . 713

[. . .]

Sección 5.ª Notificación a la persona deportista . . . 713

[. . .]

CAPÍTULO IV. Pasaporte Biológico de la persona deportista . . . 714
TÍTULO IV. Del Comité Sancionador Antidopaje . . . 715
TÍTULO V. Procedimiento para la imposición de sanciones disciplinarias en materia de dopaje . . . 715

[. . .]

CAPÍTULO II. Tramitación del procedimiento sancionador . . . 715

[. . .]

Sección 3.ª Instrucción . . . 715

[. . .]

§ 83. Ley 19/2021, de 20 de diciembre, por la que se establece el ingreso mínimo vital. [Inclusión parcial] . . . 717

[. . .]

CAPÍTULO III. Acción protectora . . . 717

[. . .]

§ 84. Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley Orgánica 8/1980, de 22 de septiembre, de Financiación de las Comunidades Autónomas y otras disposiciones conexas y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial] . . . 719

[. . .]

CAPÍTULO II. Acceso al Fichero de Titularidades Financieras por parte de las autoridades competentes . . . 719
CAPÍTULO III. Intercambio de información y análisis financieros . . . 720
CAPÍTULO IV. Protección de datos de carácter personal . . . 720

§ 85. Ley 20/2022, de 19 de octubre, de Memoria Democrática. [Inclusión parcial] . . . 723

[. . .]

Disposiciones adicionales . . . 723

§ 86. Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. [Inclusión parcial] . . . 727

[. . .]

TÍTULO II. Sistema interno de información . . . 727
CAPÍTULO I. Disposiciones generales . . . 727

[. . .]

TÍTULO VI. Protección de datos personales . . . 729

[. . .]

§ 87. Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo. [Inclusión parcial] . . . 732

LIBRO PRIMERO. Medidas de Eficiencia Digital y Procesal del Servicio Público de Justicia . . . 732
TÍTULO PRELIMINAR. Disposiciones generales . . . 732
TÍTULO I. Derechos y deberes digitales en el ámbito de la Administración de Justicia . . . 734
TÍTULO II. Acceso digital a la Administración de Justicia . . . 737
CAPÍTULO I. De la sede judicial electrónica . . . 737
CAPÍTULO II. De la Carpeta Justicia . . . 740
CAPÍTULO III. De la identificación y firma electrónicas . . . 742
Sección 1.ª Disposiciones comunes de los sistemas de identificación y firma . . . 742
Sección 2.ª Identificación y firma de la Administración de Justicia . . . 743
Sección 3.ª Interoperabilidad, identificación y representación de los ciudadanos y ciudadanas . . . 744
TÍTULO III. De la tramitación electrónica de los procedimientos judiciales . . . 745
CAPÍTULO I. Disposiciones comunes e inicio del procedimiento . . . 745

CAPÍTULO II. Tramitación orientada al dato . . . 747
CAPÍTULO III. Del documento judicial electrónico . . . 748
CAPÍTULO IV. La presentación de documentos . . . 750
CAPÍTULO V. Del expediente judicial electrónico . . . 752
CAPÍTULO VI. De las comunicaciones electrónicas . . . 753
CAPÍTULO VII. De las actuaciones automatizadas, proactivas y asistidas . . . 755
TÍTULO IV. De los actos y servicios no presenciales . . . 756
CAPÍTULO I. Actuaciones judiciales y actos y servicios no presenciales . . . 756
CAPÍTULO II. La emisión de las actuaciones celebradas por medios electrónicos . . . 759
CAPÍTULO III. Protección de datos de las actuaciones recogidas en soporte audiovisual . . . 759
CAPÍTULO IV. Seguridad de los entornos remotos de trabajo . . . 760
TÍTULO V. Los Registros de la Administración de Justicia y los archivos electrónicos . . . 760
CAPÍTULO I. Del Registro de Datos para el contacto electrónico con la Administración de Justicia . . . 760
CAPÍTULO II. Del registro de escritos . . . 761
CAPÍTULO III. Del Registro Electrónico Común de la Administración de Justicia . . . 763
CAPÍTULO IV. Del Registro Electrónico de Apoderamientos Judiciales . . . 763
CAPÍTULO V. Registro de personal al servicio de la Administración de Justicia habilitado . . . 765
CAPÍTULO VI. Archivos en la Administración de Justicia . . . 765
TÍTULO VI. Datos abiertos . . . 766
TÍTULO VII. Cooperación entre las administraciones con competencias en materia de Administración de Justicia. El Esquema Judicial de Interoperabilidad y Seguridad . . . 767
CAPÍTULO I. Marco institucional de cooperación en materia de administración electrónica. . . . 767
CAPÍTULO II. Esquema Judicial de Interoperabilidad y Seguridad . . . 768
Sección 1.ª Interoperabilidad judicial . . . 768
Sección 2.ª Ciberseguridad judicial . . . 770
CAPÍTULO III. Reutilización de aplicaciones y transferencia de tecnologías. Directorio general de información tecnológica judicial . . . 772
CAPÍTULO IV. Protección de datos de carácter personal . . . 773

[. . .]

Disposiciones adicionales . . . 773
Disposiciones transitorias . . . 775
Disposiciones derogatorias . . . 776
Disposiciones finales . . . 776
ANEXO. Definiciones . . . 776

§ 1

Constitución Española. [Inclusión parcial]

Cortes Generales
«BOE» núm. 311, de 29 de diciembre de 1978
Última modificación: 17 de febrero de 2024
Referencia: BOE-A-1978-31229

[. . .]

TÍTULO I

De los derechos y deberes fundamentales

[. . .]

CAPÍTULO SEGUNDO

Derechos y libertades

[. . .]

Sección 1.ª De los derechos fundamentales y de las libertades públicas

[. . .]

Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

[. . .]

§ 2

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Jefatura del Estado
«BOE» núm. 294, de 6 de diciembre de 2018
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2018-16673

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

PREÁMBULO

I

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus

orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva.

II

En los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. Así, se fueron adoptando en distintas instancias internacionales propuestas para la reforma del marco vigente. Y en este marco la Comisión lanzó el 4 de noviembre de 2010 su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», que constituye el germen de la posterior reforma del marco de la Unión Europea. Al propio tiempo, el Tribunal de Justicia de la Unión ha venido adoptando a lo largo de los últimos años una jurisprudencia que resulta fundamental en su interpretación.

El último hito en esta evolución tuvo lugar con la adopción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

III

El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

Asimismo, se atiende a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, los retos planteados por la rápida evolución tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información. El carácter central de la información personal tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también

riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa. Procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios. Así, el Reglamento general de protección de datos contiene un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

En este punto hay que subrayar que no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico. En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia). Por último, los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea.

La adaptación al Reglamento general de protección de datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica.

IV

Internet, por otra parte, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. Ya en los años noventa, y conscientes del impacto que iba a producir Internet en nuestras vidas, los pioneros de la Red propusieron elaborar una Declaración de los Derechos del Hombre y del Ciudadano en Internet.

Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital de nuestra

sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía.

Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.

V

Esta ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

El Título I, relativo a las disposiciones generales, comienza regulando el objeto de la ley orgánica, que es, conforme a lo que se ha indicado, doble. Así, en primer lugar, se pretende lograr la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento general de protección de datos, y completar sus disposiciones. A su vez, establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. Las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía. En segundo lugar, es también objeto de la ley garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Destaca la novedosa regulación de los datos referidos a las personas fallecidas, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido. También excluye del ámbito de aplicación los tratamientos que se rijan por disposiciones específicas, en referencia, entre otras, a la normativa que transponga la citada Directiva (UE) 2016/680, previéndose en la disposición transitoria cuarta la aplicación a estos tratamientos de la Ley Orgánica 15/1999, de 13 de diciembre, hasta que se apruebe la citada normativa.

En el Título II, «Principios de protección de datos», se establece que a efectos del Reglamento (UE) 2016/679 no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público. También se recoge expresamente el deber de confidencialidad, el tratamiento de datos amparado por la ley, las categorías especiales de datos y el tratamiento de datos de naturaleza penal, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como «consentimiento tácito», se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se mantiene en catorce años la edad a partir de la cual el menor puede prestar su consentimiento.

Se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal, Este es el caso, por ejemplo, de las bases de datos reguladas por ley y gestionadas por autoridades públicas que responden a objetivos específicos de control de riesgos y solvencia, supervisión e inspección del tipo de la Central de Información de Riesgos del Banco de España regulada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, o de los datos, documentos e informaciones de carácter reservado que obren en poder de la Dirección General de Seguros y Fondos de Pensiones de conformidad con lo previsto en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley. Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de «listas negras» de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la misma norma europea.

También en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

El Título III, dedicado a los derechos de las personas, adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Se hace uso en este Título de la habilitación permitida por el considerando 8 del Reglamento (UE) 2016/679 para complementar su régimen, garantizando la adecuada estructura sistemática del texto. A continuación, la ley orgánica contempla los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.

En el Título IV se recogen «Disposiciones aplicables a tratamientos concretos», incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de

todos los tratamientos lícitos. Dentro de ellos cabe apreciar, en primer lugar, aquellos respecto de los que el legislador establece una presunción «iuris tantum» de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este Título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general. En todo caso, el hecho de que el legislador se refiera a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa establecidas en el Capítulo IV del reglamento europeo y en el Título V de esta ley orgánica.

El Título V se refiere al responsable y al encargado del tratamiento. Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan. Con el fin de aclarar estas novedades, la ley orgánica mantiene la misma denominación del Capítulo IV del Reglamento, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las medidas generales de responsabilidad activa, al régimen del encargado del tratamiento, a la figura del delegado de protección de datos y a los mecanismos de autorregulación y certificación. La figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

El Título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El Título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la ley orgánica regula el régimen de la Agencia Española de Protección de Datos y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

El Título VIII regula el «Procedimientos en caso de posible vulneración de la normativa de protección de datos». El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de «ventanilla única» en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de

discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

La regulación se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos; y el plazo de tramitación de los procedimientos y, en su caso, su suspensión. Las especialidades del procedimiento se remiten al desarrollo reglamentario.

El Título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la ley orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el reglamento europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del Reglamento general de protección de datos.

El Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones. La ley orgánica aprovecha la cláusula residual del artículo 83.2 de la norma europea, referida a los factores agravantes o atenuantes, para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos.

Finalmente, el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Las disposiciones adicionales se refieren a cuestiones como las medidas de seguridad en el ámbito del sector público, protección de datos y transparencia y acceso a la información pública, cómputo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a prácticas abusivas que pudieran desarrollar ciertos operadores, o los tratamientos de datos de salud, entre otras.

De conformidad con la disposición adicional decimocuarta, la normativa relativa a las excepciones y limitaciones en el ejercicio de los derechos que hubiese entrado en vigor con anterioridad a la fecha de aplicación del reglamento europeo y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, seguirá vigente en tanto no sea expresamente modificada, sustituida o derogada. La pervivencia de esta normativa supone la continuidad de las excepciones y limitaciones que en ella se contienen hasta que se produzca su reforma o abrogación, si bien referida a los derechos tal y como se regulan en el Reglamento (UE) 2016/679 y en esta ley orgánica. Así, por ejemplo, en virtud de la referida disposición adicional, las Administraciones

tributarias responsables de los ficheros de datos con trascendencia tributaria a que se refiere el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, podrán, en relación con dichos datos, denegar el ejercicio de los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Las disposiciones transitorias están dedicadas, entre otras cuestiones, al estatuto de la Agencia Española de Protección de Datos, el régimen transitorio de los procedimientos o los tratamientos sometidos a la Directiva (UE) 2016/680. Se recoge una disposición derogatoria y, a continuación, figuran las disposiciones finales sobre los preceptos con carácter de ley ordinaria, el título competencial y la entrada en vigor.

Asimismo, se introducen las modificaciones necesarias de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, la Ley 14/1986, de 25 de abril, General de Sanidad, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Finalmente, y en relación con la garantía de los derechos digitales, también se introducen modificaciones en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, así como en el Texto Refundido de la Ley del Estatuto de los Trabajadores y en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la ley.*

La presente ley orgánica tiene por objeto:

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

Artículo 2. *Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94.*

1. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. Esta ley orgánica no será de aplicación:

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.

c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

3. Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

4. El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

5. El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables.

Artículo 3. *Datos de las personas fallecidas.*

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

TÍTULO II

Principios de protección de datos

Artículo 4. *Exactitud de los datos.*

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del afectado.

b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.

c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.

d) Fuesen obtenidos de un registro público por el responsable.

Artículo 5. *Deber de confidencialidad.*

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Artículo 6. *Tratamiento basado en el consentimiento del afectado.*

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

Artículo 7. *Consentimiento de los menores de edad.*

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Artículo 8. *Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.*

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos

conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Artículo 9. *Categorías especiales de datos.*

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Artículo 10. *Tratamiento de datos de naturaleza penal.*

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO III

Derechos de las personas

CAPÍTULO I

Transparencia e información

Artículo 11. *Transparencia e información al afectado.*

1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En estos supuestos, la información básica incluirá también:

a) Las categorías de datos objeto de tratamiento.
b) Las fuentes de las que procedieran los datos.

CAPÍTULO II

Ejercicio de los derechos

Artículo 12. *Disposiciones generales sobre ejercicio de los derechos.*

1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.

6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

Artículo 13. *Derecho de acceso.*

1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales

que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

Artículo 14. *Derecho de rectificación.*

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Artículo 15. *Derecho de supresión.*

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Artículo 16. *Derecho a la limitación del tratamiento.*

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.

2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Artículo 17. *Derecho a la portabilidad.*

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

Artículo 18. *Derecho de oposición.*

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

TÍTULO IV

Disposiciones aplicables a tratamientos concretos

Artículo 19. *Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.*

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

Artículo 20. *Sistemas de información crediticia.*

1. Salvo prueba en contrario, se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan los siguientes requisitos:

a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.

c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe.

La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.

d) Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

e) Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.

Cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud conforme a lo previsto en el artículo 18.1.a) del Reglamento (UE) 2016/679, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado.

f) Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

2. Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de corresponsables del tratamiento de los datos, siendo de aplicación lo establecido por el artículo 26 del Reglamento (UE) 2016/679.

Corresponderá al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.

3. La presunción a la que se refiere el apartado 1 de este artículo no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.

Artículo 21. *Tratamientos relacionados con la realización de determinadas operaciones mercantiles.*

1. Salvo prueba en contrario, se presumirán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.

2. En el caso de que la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo prevista en esta ley orgánica.

Artículo 22. *Tratamientos con fines de videovigilancia.*

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá

por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.

Artículo 23. *Sistemas de exclusión publicitaria.*

1. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados. Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas.

2. Las entidades responsables de los sistemas de exclusión publicitaria comunicarán a la autoridad de control competente su creación, su carácter general o sectorial, así como el modo en que los afectados pueden incorporarse a los mismos y, en su caso, hacer valer sus preferencias.

La autoridad de control competente hará pública en su sede electrónica una relación de los sistemas de esta naturaleza que le fueran comunicados, incorporando la información mencionada en el párrafo anterior. A tal efecto, la autoridad de control competente a la que se haya comunicado la creación del sistema lo pondrá en conocimiento de las restantes autoridades de control para su publicación por todas ellas.

3. Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, este deberá informarle de los sistemas de exclusión publicitaria existentes, pudiendo remitirse a la información publicada por la autoridad de control competente.

4. Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo. A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente.

No será necesario realizar la consulta a la que se refiere el párrafo anterior cuando el afectado hubiera prestado, conforme a lo dispuesto en esta ley orgánica, su consentimiento para recibir la comunicación a quien pretenda realizarla.

Artículo 24. *Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas.*

Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas.

Dichos tratamientos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en esta ley orgánica y en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Artículo 25. *Tratamiento de datos en el ámbito de la función estadística pública.*

1. El tratamiento de datos personales llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica, así como en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

2. La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos en que la estadística para la que se requiera la información venga exigida por una norma de

Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.

De conformidad con lo dispuesto en el artículo 11.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.

3. Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica.

Artículo 26. *Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas.*

Será lícito el tratamiento por las Administraciones Públicas de datos con fines de archivo en interés público, que se someterá a lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica con las especialidades que se derivan de lo previsto en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, así como la legislación autonómica que resulte de aplicación.

Artículo 27. *Tratamiento de datos relativos a infracciones y sanciones administrativas.*

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO V

Responsable y encargado del tratamiento

CAPÍTULO I

Disposiciones generales. Medidas de responsabilidad activa

Artículo 28. *Obligaciones generales del responsable y encargado del tratamiento.*

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización

de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Artículo 29. *Supuestos de corresponsabilidad en el tratamiento.*

La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Artículo 30. *Representantes de los responsables o encargados del tratamiento no establecidos en la Unión Europea.*

1. En los supuestos en que el Reglamento (UE) 2016/679 sea aplicable a un responsable o encargado del tratamiento no establecido en la Unión Europea en virtud de lo dispuesto en su artículo 3.2 y el tratamiento se refiera a afectados que se hallen en España, la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos podrán imponer al representante, solidariamente con el responsable o encargado del tratamiento, las medidas establecidas en el Reglamento (UE) 2016/679.

Dicha exigencia se entenderá sin perjuicio de la responsabilidad que pudiera en su caso corresponder al responsable o al encargado del tratamiento y del ejercicio por el representante de la acción de repetición frente a quien proceda.

2. Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.

Artículo 31. *Registro de las actividades de tratamiento.*

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del

Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

Artículo 32. *Bloqueo de los datos.*

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

CAPÍTULO II

Encargado del tratamiento

Artículo 33. *Encargado del tratamiento.*

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

CAPÍTULO III

Delegado de protección de datos

Artículo 34. *Designación de un delegado de protección de datos.*

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Artículo 35. *Cualificación del delegado de protección de datos.*

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Artículo 36. *Posición del delegado de protección de datos.*

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Artículo 37. *Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.*

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su

caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

CAPÍTULO IV

Códigos de conducta y certificación

Artículo 38. *Códigos de conducta.*

1. Los códigos de conducta regulados por la sección 5.ª del Capítulo IV del Reglamento (UE) 2016/679 serán vinculantes para quienes se adhieran a los mismos.

Dichos códigos podrán dotarse de mecanismos de resolución extrajudicial de conflictos.

2. Dichos códigos podrán promoverse, además de por las asociaciones y organismos a los que se refiere el artículo 40.2 del Reglamento (UE) 2016/679, por empresas o grupos de empresas así como por los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica.

Asimismo, podrán ser promovidos por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del Reglamento (UE) 2016/679.

Los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado en la reclamación, sin perjuicio de lo dispuesto en el artículo 37 de esta ley orgánica. Además, sin menoscabo de las competencias atribuidas por el Reglamento (UE) 2016/679 a las autoridades de protección de datos, podrán voluntariamente y antes de llevar a cabo el tratamiento, someter al citado organismo o entidad de supervisión la verificación de la conformidad del mismo con las materias sujetas al código de conducta.

En caso de que el organismo o entidad de supervisión rechace o desestime la reclamación, o si el responsable o encargado del tratamiento no somete la reclamación a su decisión, el afectado podrá formularla ante la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos.

La autoridad de protección de datos competente verificará que los organismos o entidades que promuevan los códigos de conducta han dotado a estos códigos de organismos de supervisión que reúnan los requisitos establecidos en el artículo 41.2 del Reglamento (UE) 2016/679.

3. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente.

4. La Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos someterán los proyectos de código al mecanismo de coherencia mencionado en el artículo 63 de Reglamento (UE) 2016/679 en los supuestos en que ello proceda según su artículo 40.7. El procedimiento quedará suspendido en tanto el

Comité Europeo de Protección de Datos no emita el dictamen al que se refieren los artículos 64.1.b) y 65.1.c) del citado reglamento.

Cuando sea una autoridad autonómica de protección de datos la que someta el proyecto de código al mecanismo de coherencia, se estará a lo dispuesto en el artículo 60 de esta ley orgánica.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos conforme al artículo 40.11 del citado reglamento.

El registro será accesible a través de medios electrónicos.

6. Mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.

Artículo 39. *Acreditación de instituciones de certificación.*

Sin perjuicio de las funciones y poderes de acreditación de la autoridad de control competente en virtud de los artículos 57 y 58 del Reglamento (UE) 2016/679, la acreditación de las instituciones de certificación a las que se refiere el artículo 43.1 del citado reglamento podrá ser llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

TÍTULO VI

Transferencias internacionales de datos

Artículo 40. *Régimen de las transferencias internacionales de datos.*

Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias.

En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.

Artículo 41. *Supuestos de adopción por la Agencia Española de Protección de Datos.*

1. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del citado reglamento.

2. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.

El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, y continuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente.

Artículo 42. *Supuestos sometidos a autorización previa de las autoridades de protección de datos.*

1. Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse en los siguientes supuestos:

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

El procedimiento tendrá una duración máxima de seis meses.

2. La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refieren los artículos 64.1.e), 64.1.f) y 65.1.c) del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia Española de Protección de Datos o, por conducto de la misma, a la autoridad de control competente, en su caso.

Artículo 43. *Supuestos sometidos a información previa a la autoridad de protección de datos competente.*

Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos.

Esta información deberá facilitarse con carácter previo a la realización de la transferencia.

Lo dispuesto en este artículo no será de aplicación a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos, de acuerdo con el artículo 49.3 del Reglamento (UE) 2016/679.

TÍTULO VII

Autoridades de protección de datos

CAPÍTULO I

La Agencia Española de Protección de Datos

Sección 1.ª Disposiciones generales

Artículo 44. *Disposiciones generales.*

1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Se relaciona con el Gobierno a través del Ministerio de Justicia.

2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.

3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

Artículo 45. *Régimen jurídico.*

1. La Agencia Española de Protección de Datos se rige por lo dispuesto en el Reglamento (UE) 2016/679, la presente ley orgánica y sus disposiciones de desarrollo.

Supletoriamente, en cuanto sea compatible con su plena independencia y sin perjuicio de lo previsto en el artículo 63.2 de esta ley orgánica, se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto mediante real decreto.

Artículo 46. *Régimen económico presupuestario y de personal.*

1. La Agencia Española de Protección de Datos elaborará y aprobará su presupuesto y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado.

2. El régimen de modificaciones y de vinculación de los créditos de su presupuesto será el establecido en el Estatuto de la Agencia Española de Protección de Datos.

Corresponde a la Presidencia de la Agencia Española de Protección de Datos autorizar las modificaciones presupuestarias que impliquen hasta un tres por ciento de la cifra inicial de su presupuesto total de gastos, siempre que no se incrementen los créditos para gastos de personal. Las restantes modificaciones que no excedan de un cinco por ciento del presupuesto serán autorizadas por el Ministerio de Hacienda y, en los demás casos, por el Gobierno.

3. La Agencia Española de Protección de Datos contará para el cumplimiento de sus fines con las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado, los bienes y valores que constituyan su patrimonio y los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidos en el artículo 58 del Reglamento (UE) 2016/679.

4. El resultado positivo de sus ingresos se destinará por la Agencia Española de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia.

5. El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral y se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normativa reguladora de los funcionarios públicos y, en su caso, por la normativa laboral.

6. La Agencia Española de Protección Datos elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto. En dicha relación de puestos de trabajo constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas.

7. Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, la gestión económico-financiera de la Agencia Española de Protección de Datos estará sometida al

control de la Intervención General de la Administración del Estado en los términos que establece la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Artículo 47. *Funciones y potestades de la Agencia Española de Protección de Datos.*

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Artículo 48. *La Presidencia de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

2. La Presidencia de la Agencia Española de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones, a excepción de las relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado.

En los supuestos de ausencia, vacante o enfermedad de la persona titular de la Presidencia o cuando concurran en ella alguno de los motivos de abstención o recusación previstos en el artículo 23 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el ejercicio de las competencias relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica serán asumidas por la persona titular del órgano directivo que desarrolle las funciones de inspección. En el supuesto de que cualquiera de las circunstancias mencionadas concurriera igualmente en dicha persona, el ejercicio de las competencias afectadas será asumido por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

El ejercicio del resto de competencias será asumido por el Adjunto en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos y, en su defecto, por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

3. La Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

4. La Presidencia y el Adjunto de la Agencia Española de Protección de Datos serán nombrados por el Consejo de Ministros mediante real decreto.

5. El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de cinco años y puede ser renovado para otro período de igual duración.

La Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por:

a) Incumplimiento grave de sus obligaciones,
b) incapacidad sobrevenida para el ejercicio de su función,
c) incompatibilidad, o
d) condena firme por delito doloso.

En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas en el apartado 3 de este artículo.

6. Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

Artículo 49. *Consejo Consultivo de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos estará asesorada por un Consejo Consultivo compuesto por los siguientes miembros:

a) Un Diputado, propuesto por el Congreso de los Diputados.
b) Un Senador, propuesto por el Senado.
c) Un representante designado por el Consejo General del Poder Judicial.
d) Un representante de la Administración General del Estado con experiencia en la materia, propuesto por el Ministro de Justicia.
e) Un representante de cada Comunidad Autónoma que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma.
f) Un experto propuesto por la Federación Española de Municipios y Provincias.
g) Un experto propuesto por el Consejo de Consumidores y Usuarios.
h) Dos expertos propuestos por las Organizaciones Empresariales.
i) Un representante de los profesionales de la protección de datos y de la privacidad, propuesto por la asociación de ámbito estatal con mayor número de asociados.
j) Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos previstos en el Capítulo IV del Título V, propuesto por el Ministro de Justicia.
k) Un experto, propuesto por la Conferencia de Rectores de las Universidades Españolas.
l) Un representante de las organizaciones que agrupan a los Consejos Generales, Superiores y Colegios Profesionales de ámbito estatal de las diferentes profesiones colegiadas, propuesto por el Ministro de Justicia.
m) Un representante de los profesionales de la seguridad de la información, propuesto por la asociación de ámbito estatal con mayor número de asociados.
n) Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno.
ñ) Dos expertos propuestos por las organizaciones sindicales más representativas.

2. A los efectos del apartado anterior, la condición de experto requerirá acreditar conocimientos especializados en el Derecho y la práctica en materia de protección de datos mediante el ejercicio profesional o académico.

3. Los miembros del Consejo Consultivo serán nombrados por orden del Ministro de Justicia, publicada en el Boletín Oficial del Estado.

4. El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al semestre.

5. Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante.

6. En todo lo no previsto por esta ley orgánica, el régimen, competencias y funcionamiento del Consejo Consultivo serán los establecidos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Artículo 50. *Publicidad.*

La Agencia Española de Protección de Datos publicará las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los

artículos 15 a 22 del Reglamento (UE) 2016/679, las que pongan fin a los procedimientos sancionadores y a los procedimientos de apercibimiento, las que archiven las actuaciones previas de investigación, las dictadas respecto de las entidades a que se refiere el artículo 77.1 de esta ley orgánica, las que impongan medidas cautelares y las demás que disponga su Estatuto.

Sección 2.ª Potestades de investigación y planes de auditoría preventiva

Artículo 51. *Ámbito y personal competente.*

1. La Agencia Española de Protección de Datos desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII y de los planes de auditoría preventivas.

2. La actividad de investigación se llevará a cabo por los funcionarios de la Agencia Española de Protección de Datos o por funcionarios ajenos a ella habilitados expresamente por su Presidencia.

3. En los casos de actuaciones conjuntas de investigación conforme a lo dispuesto en el artículo 62 del Reglamento (UE) 2016/679, el personal de las autoridades de control de otros Estados Miembros de Unión Europea que colabore con la Agencia Española de Protección de Datos ejercerá sus facultades con arreglo a lo previsto en la presente ley orgánica y bajo la orientación y en presencia del personal de esta.

4. Los funcionarios que desarrollen actividades de investigación tendrán la consideración de agentes de la autoridad en el ejercicio de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio, incluso después de haber cesado en él.

Artículo 52. *Deber de colaboración.*

1. Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación.

Cuando la información contenga datos personales la comunicación de dichos datos estará amparada por lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679.

2. En el marco de las actuaciones previas de investigación, cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, las informaciones y datos que resulten imprescindibles con la exclusiva finalidad de lograr la identificación de los responsables de las conductas que pudieran ser constitutivas de infracción del Reglamento (UE) 2016/679 y de la presente ley orgánica.

En el supuesto de las Administraciones tributarias y de la Seguridad Social, la información se limitará a la que resulte necesaria para poder identificar inequívocamente contra quién debe dirigirse la actuación de la Agencia Española de Protección de Datos en los supuestos de creación de entramados societarios que dificultasen el conocimiento directo del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica.

3. Cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información los datos que obren en su poder y que resulten imprescindibles para la identificación del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica cuando se hubiere llevado a cabo mediante la utilización de un servicio de la sociedad de la información o la realización de una comunicación electrónica. A tales efectos, los datos que la Agencia Española de Protección de Datos podrá recabar al amparo de este apartado son los siguientes:

a) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de telefonía fija o móvil:

1.º El número de teléfono de origen de la llamada en caso de que el mismo se hubiese ocultado.

2.º El nombre, número de documento identificativo y dirección del abonado o usuario registrado al que corresponda ese número de teléfono.

3.º La mera confirmación de que se ha realizado una llamada específica entre dos números en una determinada fecha y hora.

b) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de la sociedad de la información:

1.º La identificación de la dirección de protocolo de Internet desde la que se hubiera llevado a cabo la conducta y la fecha y hora de su realización.

2.º Si la conducta se hubiese llevado a cabo mediante correo electrónico, la identificación de la dirección de protocolo de Internet desde la que se creó la cuenta de correo y la fecha y hora en que la misma fue creada.

3.º El nombre, número de documento identificativo y dirección del abonado o del usuario registrado al que se le hubiera asignado la dirección de Protocolo de Internet a la que se refieren los dos párrafos anteriores.

Estos datos deberán ser cedidos, previo requerimiento motivado de la Agencia Española de Protección de Datos, exclusivamente en el marco de actuaciones de investigación iniciadas como consecuencia de una denuncia presentada por un afectado respecto de una conducta de una persona jurídica o respecto a la utilización de sistemas que permitan la divulgación sin restricciones de datos personales. En el resto de los supuestos la cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales cuando resultara exigible.

Quedan excluidos de lo previsto en este apartado los datos de tráfico que los operadores estuviesen tratando con la exclusiva finalidad de dar cumplimiento a las obligaciones previstas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuya cesión solamente podrá tener lugar de acuerdo con lo dispuesto en ella, previa autorización judicial solicitada por alguno de los agentes facultados a los que se refiere el artículo 6 de dicha ley.

Artículo 53. *Alcance de la actividad de investigación.*

1. Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos necesarios, examinarlos en el lugar en que se encuentren depositados o en donde se lleven a cabo los tratamientos, obtener copia de ellos, inspeccionar los equipos físicos y lógicos y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación.

2. Cuando fuese necesario el acceso por el personal que desarrolla la actividad de investigación al domicilio constitucionalmente protegido del inspeccionado, será preciso contar con su consentimiento o haber obtenido la correspondiente autorización judicial.

3. Cuando se trate de órganos judiciales u oficinas judiciales el ejercicio de las facultades de inspección se efectuará a través y por mediación del Consejo General del Poder Judicial.

Artículo 53 bis. *Actuaciones de investigación a través de sistemas digitales.*

Las actuaciones de investigación podrán realizarse a través de sistemas digitales que, mediante la videoconferencia u otro sistema similar, permitan la comunicación bidireccional y simultánea de imagen y sonido, la interacción visual, auditiva y verbal entre la Agencia Española de Protección de Datos y el inspeccionado. Además, deben garantizar la transmisión y recepción seguras de los documentos e información que se intercambien, y, en su caso, recoger las evidencias necesarias y el resultado de las actuaciones realizadas asegurando su autoría, autenticidad e integridad.

La utilización de estos sistemas se producirá cuando lo determine la Agencia y requerirá la conformidad del inspeccionado en relación con su uso y con la fecha y hora de su desarrollo.

Artículo 54. *Planes de auditoría.*

1. La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones del Reglamento (UE) 2016/679 y de la presente ley orgánica, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.

2. A resultas de los planes de auditoría, la Presidencia de la Agencia Española de Protección de Datos podrá dictar las directrices generales o específicas para un concreto responsable o encargado de los tratamientos precisas para asegurar la plena adaptación del sector o responsable al Reglamento (UE) 2016/679 y a la presente ley orgánica.

En la elaboración de dichas directrices la Presidencia de la Agencia Española de Protección de Datos podrá solicitar la colaboración de los organismos de supervisión de los códigos de conducta y de resolución extrajudicial de conflictos, si los hubiere.

3. Las directrices serán de obligado cumplimiento para el sector o responsable al que se refiera el plan de auditoría.

Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos

Artículo 55. *Potestades de regulación. Circulares de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, que se denominarán «Circulares de la Agencia Española de Protección de Datos».

2. Su elaboración se sujetará al procedimiento establecido en el Estatuto de la Agencia Española de Protección de Datos, que deberá prever los informes técnicos y jurídicos que fueran necesarios y la audiencia a los interesados.

3. Las circulares serán obligatorias una vez publicadas en el Boletín Oficial del Estado.

Artículo 56. *Acción exterior.*

1. Corresponde a la Agencia Española de Protección de Datos la titularidad y el ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos.

Asimismo a las comunidades autónomas, a través de las autoridades autonómicas de protección de datos, les compete ejercitar las funciones como sujetos de la acción exterior en el marco de sus competencias de conformidad con lo dispuesto en la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado, así como celebrar acuerdos internacionales administrativos en ejecución y concreción de un tratado internacional y acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, no vinculantes jurídicamente para quienes los suscriben, sobre materias de su competencia en el marco de la Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales.

2. La Agencia Española de Protección de Datos es el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier Convenio Internacional en el que sea parte el Reino de España que atribuya a una autoridad nacional de control esa competencia y la representante común de las autoridades de Protección de Datos en el Comité Europeo de Protección de Datos, conforme a lo dispuesto en el artículo 68.4 del Reglamento (UE) 2016/679.

La Agencia Española de Protección de Datos informará a las autoridades autonómicas de protección de datos acerca de las decisiones adoptadas en el Comité Europeo de Protección de Datos y recabará su parecer cuando se trate de materias de su competencia.

3. Sin perjuicio de lo dispuesto en el apartado 1, la Agencia Española de Protección de Datos:

a) Participará en reuniones y foros internacionales de ámbito distinto al de la Unión Europea establecidos de común acuerdo por las autoridades de control independientes en materia de protección de datos.

b) Participará, como autoridad española, en las organizaciones internacionales competentes en materia de protección de datos, en los comités o grupos de trabajo, de estudio y de colaboración de organizaciones internacionales que traten materias que afecten al derecho fundamental a la protección de datos personales y en otros foros o grupos de trabajo internacionales, en el marco de la acción exterior del Estado.

c) Colaborará con autoridades, instituciones, organismos y Administraciones de otros Estados a fin de impulsar, promover y desarrollar el derecho fundamental a la protección de datos, en particular en el ámbito iberoamericano, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia.

CAPÍTULO II

Autoridades autonómicas de protección de datos

Sección 1.ª Disposiciones generales

Artículo 57. *Autoridades autonómicas de protección de datos.*

1. Las autoridades autonómicas de protección de datos personales podrán ejercer, las funciones y potestades establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679, de acuerdo con la normativa autonómica, cuando se refieran a:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

2. Las autoridades autonómicas de protección de datos podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para la Agencia Española de Protección de Datos en el artículo 55 de esta ley orgánica.

Artículo 58. *Cooperación institucional.*

La Presidencia de la Agencia Española de Protección de Datos convocará, por iniciativa propia o cuando lo solicite otra autoridad, a las autoridades autonómicas de protección de datos para contribuir a la aplicación coherente del Reglamento (UE) 2016/679 y de la presente ley orgánica. En todo caso, se celebrarán reuniones semestrales de cooperación.

La Presidencia de la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán solicitar y deberán intercambiarse mutuamente la información necesaria para el cumplimiento de sus funciones y, en particular, la relativa a la actividad del Comité Europeo de Protección de Datos. Asimismo, podrán constituir grupos de trabajo para tratar asuntos específicos de interés común.

Artículo 59. *Tratamientos contrarios al Reglamento (UE) 2016/679.*

Cuando la Presidencia de la Agencia Española de Protección de Datos considere que un tratamiento llevado a cabo en materias que fueran competencia de las autoridades autonómicas de protección de datos vulnera el Reglamento (UE) 2016/679 podrá requerirlas a que adopten, en el plazo de un mes, las medidas necesarias para su cesación.

Si la autoridad autonómica no atendiere en plazo el requerimiento o las medidas adoptadas no supusiesen la cesación en el tratamiento ilícito, la Agencia Española de

Protección de Datos podrá ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.

Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679

Artículo 60. *Coordinación en caso de emisión de dictamen por el Comité Europeo de Protección de Datos.*

Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando éstas, como autoridades competentes, deban someter su proyecto de decisión al citado comité o le soliciten el examen de un asunto en virtud de lo establecido en los apartados 1 y 2 del artículo 64 del Reglamento (UE) 2016/679.

En estos casos, la Agencia Española de Protección de Datos será asistida por un representante de la Autoridad autonómica en su intervención ante el Comité.

Artículo 61. *Intervención en caso de tratamientos transfronterizos.*

1. Las autoridades autonómicas de protección de datos ostentarán la condición de autoridad de control principal o interesada en el procedimiento establecido por el artículo 60 del Reglamento (UE) 2016/679 cuando se refiera a un tratamiento previsto en el artículo 57 de esta ley orgánica que se llevara a cabo por un responsable o encargado del tratamiento de los previstos en el artículo 56 del Reglamento (UE) 2016/679, salvo que desarrollase significativamente tratamientos de la misma naturaleza en el resto del territorio español.

2. Corresponderá en estos casos a las autoridades autonómicas intervenir en los procedimientos establecidos en el artículo 60 del Reglamento (UE) 2016/679, informando a la Agencia Española de Protección de Datos sobre su desarrollo en los supuestos en que deba aplicarse el mecanismo de coherencia.

Artículo 62. *Coordinación en caso de resolución de conflictos por el Comité Europeo de Protección de Datos.*

1. Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando estas, como autoridades principales, deban solicitar del citado Comité la emisión de una decisión vinculante según lo previsto en el artículo 65 del Reglamento (UE) 2016/679.

2. Las autoridades autonómicas de protección de datos que tengan la condición de autoridad interesada no principal en un procedimiento de los previstos en el artículo 65 del Reglamento (UE) 2016/679 informarán a la Agencia Española de Protección de Datos cuando el asunto sea remitido al Comité Europeo de Protección de Datos, facilitándole la documentación e información necesarias para su tramitación.

La Agencia Española de Protección de Datos será asistida por un representante de la autoridad autonómica interesada en su intervención ante el mencionado comité.

TÍTULO VIII

Procedimientos en caso de posible vulneración de la normativa de protección de datos

Artículo 63. *Régimen jurídico.*

1. Las disposiciones de este Título serán de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquella investigue la existencia de una posible infracción de lo dispuesto en el mencionado reglamento y en la presente ley orgánica.

2. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

3. El Gobierno regulará por real decreto los procedimientos que tramite la Agencia Española de Protección de Datos al amparo de este Título, asegurando en todo caso los derechos de defensa y audiencia de los interesados.

Artículo 64. *Forma de iniciación del procedimiento y duración.*

1. Cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se iniciará por acuerdo de admisión a trámite, que se adoptará conforme a lo establecido en el artículo 65 de esta ley orgánica.

En este caso el plazo para resolver el procedimiento será de seis meses a contar desde la fecha en que hubiera sido notificado al reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación.

2. Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la presente ley orgánica, se iniciará mediante acuerdo de inicio, adoptado por propia iniciativa o como consecuencia de reclamación, que le será notificado al interesado.

Si el procedimiento se fundase en una reclamación formulada ante la Agencia Española de Protección de Datos, con carácter previo, esta decidirá sobre su admisión a trámite, conforme a lo dispuesto en el artículo 65 de esta ley orgánica.

Admitida a trámite la reclamación, así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 67 de esta ley orgánica.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

3. Cuando así proceda en atención a la naturaleza de los hechos y teniendo debidamente en cuenta los criterios establecidos en el artículo 83.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Agencia Española de Protección de Datos, previa audiencia al responsable o encargado del tratamiento, podrá dirigir un apercibimiento, así como ordenar al responsable o encargado del tratamiento que adopten las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos de una determinada manera y dentro del plazo especificado.

El procedimiento tendrá una duración máxima de seis meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

Será de aplicación en este caso lo dispuesto en los párrafos segundo y tercero del apartado 2 de este artículo.

4. El procedimiento podrá también tramitarse como consecuencia de la comunicación a la Agencia Española de Protección de Datos por parte de la autoridad de control de otro Estado miembro de la Unión Europea de la reclamación formulada ante la misma, cuando la Agencia Española de Protección de Datos tuviese la condición de autoridad de control principal para la tramitación de un procedimiento conforme a lo dispuesto en los artículos 56 y 60 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Será en este caso de aplicación lo dispuesto en los apartados 1, 2 y 3 de este artículo.

5. Los plazos de tramitación establecidos en este artículo así como los de admisión a trámite regulados por el artículo 65.5 y de duración de las actuaciones previas de investigación previstos en el artículo 67.2, quedarán automáticamente suspendidos cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de un órgano u organismo de la Unión Europea o de una o varias autoridades de control de

los Estados miembros conforme con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Agencia Española de Protección de Datos.

6. El transcurso de los plazos de tramitación a los que se refiere el apartado anterior se podrá suspender, mediante resolución motivada, cuando resulte indispensable recabar información de un órgano jurisdiccional.

Artículo 65. *Admisión a trámite de las reclamaciones.*

1. Cuando se presentase ante la Agencia Española de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.

2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

3. Igualmente, la Agencia Española de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia Española de Protección de Datos, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado en el caso de las infracciones previstas en el artículo 74 de esta ley orgánica.

b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá remitir la misma al delegado de protección de datos que hubiera, en su caso, designado el responsable o encargado del tratamiento, al organismo de supervisión establecido para la aplicación de los códigos de conducta o al organismo que asuma las funciones de resolución extrajudicial de conflictos a los efectos previstos en los artículos 37 y 38.2 de esta ley orgánica.

La Agencia Española de Protección de Datos podrá igualmente remitir la reclamación al responsable o encargado del tratamiento cuando no se hubiera designado un delegado de protección de datos ni estuviera adherido a mecanismos de resolución extrajudicial de conflictos, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación en el plazo de un mes.

Si como consecuencia de dichas actuaciones de remisión, el responsable o encargado del tratamiento demuestra haber adoptado medidas para el cumplimiento de la normativa aplicable, la Agencia Española de Protección de Datos podrá inadmitir a trámite la reclamación.

5. La decisión sobre la admisión o inadmisión a trámite, así como la que determine, en su caso, la remisión de la reclamación a la autoridad de control principal que se estime competente, deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación con arreglo a lo dispuesto en este título a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia Española de Protección de Datos, sin perjuicio de la facultad de la Agencia de archivar posteriormente y de forma expresa la reclamación.

En el supuesto de que la Agencia Española de Protección de Datos actúe como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.4 de esta ley orgánica, el cómputo del plazo señalado en el párrafo anterior se iniciará una vez que se reciba en la Agencia toda la documentación necesaria para su tramitación.

Cuando los hechos de una reclamación relativa a la posible existencia en el ámbito competencial de la Agencia, guarden identidad sustancial con los que sean objeto de unas actuaciones previas de investigación o de un procedimiento sancionador ya iniciado, en la notificación de la decisión de admisión a trámite se podrá indicar el número de expediente

correspondiente a las actuaciones previas o al procedimiento correspondiente, así como de la dirección web en la que se publicará la resolución que ponga fin al mismo, a efectos de que el reclamante pueda conocer el curso y resultado de la investigación.

6. Tras la admisión a trámite, si el responsable o encargado del tratamiento demuestran haber adoptado medidas para el cumplimiento de la normativa aplicable, la Agencia Española de Protección de Datos podrá resolver el archivo de la reclamación, cuando en el caso concreto concurran circunstancias que aconsejen la adopción de otras soluciones más moderadas o alternativas a la acción correctiva, siempre que no se hayan iniciado actuaciones previas de investigación o alguno de los procedimientos regulados en esta ley orgánica.

Artículo 66. *Determinación del alcance territorial.*

1. Salvo en los supuestos a los que se refiere el artículo 64.4 de esta ley orgánica, la Agencia Española de Protección de Datos deberá, con carácter previo a la realización de cualquier otra actuación, incluida la admisión a trámite de una reclamación o el comienzo de actuaciones previas de investigación, examinar su competencia y determinar el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir.

2. Si la Agencia Española de Protección de Datos considera que no tiene la condición de autoridad de control principal para la tramitación del procedimiento remitirá, sin más trámite, la reclamación formulada a la autoridad de control principal que considere competente, a fin de que por la misma se le dé el curso oportuno. La Agencia Española de Protección de Datos notificará esta circunstancia a quien, en su caso, hubiera formulado la reclamación.

El acuerdo por el que se resuelva la remisión a la que se refiere el párrafo anterior implicará el archivo provisional del procedimiento, sin perjuicio de que por la Agencia Española de Protección de Datos se dicte, en caso de que así proceda, la resolución a la que se refiere el apartado 8 del artículo 60 del Reglamento (UE) 2016/679.

Artículo 67. *Actuaciones previas de investigación.*

1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en la sección 2.ª del capítulo I del título VII de esta ley orgánica y no podrán tener una duración superior a dieciocho meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa.

Artículo 68. *Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora.*

1. Concluidas, en su caso, las actuaciones a las que se refiere el artículo anterior, corresponderá a la Presidencia de la Agencia Española de Protección de Datos, cuando así proceda, dictar acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, en que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

2. Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679, el proyecto de acuerdo de inicio de procedimiento sancionador se someterá a lo dispuesto en el mismo.

Artículo 69. *Medidas provisionales y de garantía de los derechos.*

1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de

Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.

2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia Española de Protección de Datos una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.

TÍTULO IX

Régimen sancionador

Artículo 70. *Sujetos responsables.*

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

a) Los responsables de los tratamientos.
b) Los encargados de los tratamientos.
c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.
d) Las entidades de certificación.
e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título.

Artículo 71. *Infracciones.*

Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.

Artículo 72. *Infracciones consideradas muy graves.*

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.
b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.
c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento.
d) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica.

f) El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 10 de esta ley orgánica.

g) El tratamiento de datos personales relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 27 de esta ley orgánica.

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica.

i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica.

j) La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.

k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

l) La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679.

m) El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 32 de esta ley orgánica cuando la misma sea exigible.

ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

p) La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

2. Tendrán la misma consideración y también prescribirán a los tres años las infracciones a las que se refiere el artículo 83.6 del Reglamento (UE) 2016/679.

Artículo 73. *Infracciones consideradas graves.*

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del Reglamento (UE) 2016/679.

b) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del Reglamento (UE) 2016/679.

c) El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el

diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.

e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.

h) El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.

i) La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.

j) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del Reglamento (UE) 2016/679.

k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

l) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

m) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

n) No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679.

ñ) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del Reglamento (UE) 2016/679.

o) No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.

p) El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 28 de esta ley orgánica.

q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

s) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

u) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del Reglamento (UE) 2016/679 o cuando la ley establezca la obligación de llevar a cabo esa consulta.

v) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

w) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

x) La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado.

y) Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del Reglamento (UE) 2016/679.

z) El desempeño de funciones que el Reglamento (UE) 2016/679 reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 39 de esta ley orgánica.

aa) El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 42 y 43 de Reglamento (UE) 2016/679.

ab) El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.

ac) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 74. *Infracciones consideradas leves.*

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.

b) La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.

c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de esta ley orgánica.

d) No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73 c) de esta ley orgánica.

e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del Reglamento (UE) 2016/679.

f) El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3 de esta ley orgánica.

h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al

tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE) 2016/679 o la inexactitud en la determinación de las mismas.

i) No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.

j) La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de este de las disposiciones del Reglamento (UE) 2016/679 o de esta ley orgánica, conforme a lo exigido por el artículo 28.3 del citado reglamento.

k) El incumplimiento por el encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al Reglamento (UE) 2016/679 y a la presente ley orgánica o en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

l) Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del Reglamento (UE) 2016/679.

m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de documentar cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica.

o) Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.

p) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

q) El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme a lo exigido por los apartados 1 y 5 del artículo 43 del Reglamento (UE) 2016/679.

r) El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 75. *Interrupción de la prescripción de la infracción.*

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del acuerdo de inicio.

Artículo 76. *Sanciones y medidas correctivas.*

1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.
4. Será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción fuese superior a un millón de euros y el infractor sea una persona jurídica.
Cuando la autoridad competente para imponer la sanción sea una autoridad autonómica de protección de datos, se estará a su normativa de aplicación.

Artículo 77. *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.*

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica.

Artículo 78. *Prescripción de las sanciones.*

1. Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 y de esta ley orgánica prescriben en los siguientes plazos:

a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año.

b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.

c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

3. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

TÍTULO X

Garantía de los derechos digitales

Artículo 79. *Los derechos en la Era digital.*

Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.

Artículo 80. *Derecho a la neutralidad de Internet.*

Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

Artículo 81. *Derecho de acceso universal a Internet.*

1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.

2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.

3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.

4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.

5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.

6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

Artículo 82. *Derecho a la seguridad digital.*

Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.

Artículo 83. *Derecho a la educación digital.*

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las Administraciones educativas deberán incluir en el desarrollo del currículo la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

Artículo 84. *Protección de los menores en Internet.*

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

Artículo 85. *Derecho de rectificación en Internet.*

1. Todos tienen derecho a la libertad de expresión en Internet.

2. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

Artículo 86. *Derecho a la actualización de informaciones en medios de comunicación digitales.*

Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.

Artículo 87. *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Artículo 88. *Derecho a la desconexión digital en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia

así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Artículo 89. *Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.*

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

Artículo 90. *Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.*

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Artículo 91. *Derechos digitales en la negociación colectiva.*

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

Artículo 92. *Protección de datos de los menores en Internet.*

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

Artículo 93. *Derecho al olvido en búsquedas de Internet.*

1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Artículo 94. *Derecho al olvido en servicios de redes sociales y servicios equivalentes.*

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

Artículo 95. *Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.*

Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

Artículo 96. *Derecho al testamento digital.*

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al

objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

Artículo 97. *Políticas de impulso de los derechos digitales.*

1. El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público; y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

2. Asimismo se aprobará un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

3. El Gobierno presentará un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías y mandatos contemplados en el presente Título y de las medidas necesarias para promover su impulso y efectividad.

Disposición adicional primera. *Medidas de seguridad en el ámbito del sector público.*

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Disposición adicional segunda. *Protección de datos y transparencia y acceso a la información pública.*

La publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición adicional tercera. *Cómputo de plazos.*

Los plazos establecidos en el Reglamento (UE) 2016/679 o en esta ley orgánica, con independencia de que se refieran a relaciones entre particulares o con entidades del sector público, se regirán por las siguientes reglas:

a) Cuando los plazos se señalen por días, se entiende que estos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos.

b) Si el plazo se fija en semanas, concluirá el mismo día de la semana en que se produjo el hecho que determina su iniciación en la semana de vencimiento.

c) Si el plazo se fija en meses o años, concluirá el mismo día en que se produjo el hecho que determina su iniciación en el mes o el año de vencimiento. Si en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entenderá que el plazo expira el último día del mes.

d) Cuando el último día del plazo sea inhábil, se entenderá prorrogado al primer día hábil siguiente.

Disposición adicional cuarta. *Procedimiento en relación con las competencias atribuidas a la Agencia Española de Protección de Datos por otras leyes.*

Lo dispuesto en el Título VIII y en sus normas de desarrollo será de aplicación a los procedimientos que la Agencia Española de Protección de Datos hubiera de tramitar en ejercicio de las competencias que le fueran atribuidas por otras leyes.

Disposición adicional quinta. *Autorización judicial en relación con decisiones de la Comisión Europea en materia de transferencia internacional de datos.*

1. Cuando una autoridad de protección de datos considerase que una decisión de la Comisión Europea en materia de transferencia internacional de datos, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el Reglamento (UE) 2016/679, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente la suspensión del procedimiento, a fin de solicitar del órgano judicial autorización para declararlo así en el seno del procedimiento del que esté conociendo. Dicha suspensión deberá ser confirmada, modificada o levantada en el acuerdo de admisión o inadmisión a trámite de la solicitud de la autoridad de protección de datos dirigida al tribunal competente.

Las decisiones de la Comisión Europea a las que puede resultar de aplicación este cauce son:

a) aquellas que declaren el nivel adecuado de protección de un tercer país u organización internacional, en virtud del artículo 45 del Reglamento (UE) 2016/679;

b) aquellas por las que se aprueben cláusulas tipo de protección de datos para la realización de transferencias internacionales de datos, o

c) aquellas que declaren la validez de los códigos de conducta a tal efecto.

2. La autorización a la que se refiere esta disposición solamente podrá ser concedida si, previo planteamiento de cuestión prejudicial de validez en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea, la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

Disposición adicional sexta. *Incorporación de deudas a sistemas de información crediticia.*

No se incorporarán a los sistemas de información crediticia a los que se refiere el artículo 20.1 de esta ley orgánica deudas en que la cuantía del principal sea inferior a cincuenta euros.

El Gobierno, mediante real decreto, podrá actualizar esta cuantía.

Disposición adicional séptima. *Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.*

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

Disposición adicional octava. *Potestad de verificación de las Administraciones Públicas.*

Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

Disposición adicional novena. *Tratamiento de datos personales en relación con la notificación de incidentes de seguridad.*

Cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante

incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

Disposición adicional décima. *Comunicaciones de datos por los sujetos enumerados en el artículo 77.1.*

Los responsables enumerados en el artículo 77.1 de esta ley orgánica podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679.

Disposición adicional undécima. *Privacidad en las comunicaciones electrónicas.*

Lo dispuesto en la presente ley orgánica se entenderá sin perjuicio de la aplicación de las normas de Derecho interno y de la Unión Europea reguladoras de la privacidad en el sector de las comunicaciones electrónicas, sin imponer obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación en ámbitos en los que estén sujetas a obligaciones específicas establecidas en dichas normas.

Disposición adicional duodécima. *Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.*

1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.

2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.

3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

Disposición adicional decimotercera. *Transferencias internacionales de datos tributarios.*

Las transferencias de datos tributarios entre el Reino de España y otros Estados o entidades internacionales o supranacionales, se regularán por los términos y con los límites establecidos en la normativa sobre asistencia mutua entre los Estados de la Unión Europea, o en el marco de los convenios para evitar la doble imposición o de otros convenios internacionales, así como por las normas sobre la asistencia mutua establecidas en el Capítulo VI del Título III de la Ley 58/2003, de 17 de diciembre, General Tributaria.

Disposición adicional decimocuarta. *Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE.*

Las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.

Disposición adicional decimoquinta. *Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores.*

Cuando no haya podido obtener por otros medios la información necesaria para realizar sus labores de supervisión e inspección relacionadas con la detección de delitos graves, la Comisión Nacional del Mercado de Valores podrá recabar de los operadores que presten

servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, los datos que obren en su poder relativos a la comunicación electrónica o servicio de la sociedad de la información proporcionados por dichos prestadores que sean distintos a su contenido y resulten imprescindibles para el ejercicio de dichas labores.

La cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales.

Disposición adicional decimosexta. *Prácticas agresivas en materia de protección de datos.*

A los efectos previstos en el artículo 8 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, se consideran prácticas agresivas las siguientes:

a) Actuar con intención de suplantar la identidad de la Agencia Española de Protección de Datos o de una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos o a los interesados.

b) Generar la apariencia de que se está actuando en nombre, por cuenta o en colaboración con la Agencia Española de Protección de Datos o una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos en que la remitente ofrezca sus productos o servicios.

c) Realizar prácticas comerciales en las que se coarte el poder de decisión de los destinatarios mediante la referencia a la posible imposición de sanciones por incumplimiento de la normativa de protección de datos personales.

d) Ofrecer cualquier tipo de documento por el que se pretenda crear una apariencia de cumplimiento de las disposiciones de protección de datos de forma complementaria a la realización de acciones formativas sin haber llevado a cabo las actuaciones necesarias para verificar que dicho cumplimiento se produce efectivamente.

e) Asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos.

Disposición adicional decimoséptima. *Tratamientos de datos de salud.*

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:

1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.

2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.

3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Disposición adicional decimoctava. *Criterios de seguridad.*

La Agencia Española de Protección de Datos desarrollará, con la colaboración, cuando sea precisa, de todos los actores implicados, las herramientas, guías, directrices y orientaciones que resulten precisas para dotar a los profesionales, microempresas y pequeñas y medianas empresas de pautas adecuadas para el cumplimiento de las obligaciones de responsabilidad activa establecidas en el Título IV del Reglamento (UE) 2016/679 y en el Título V de esta ley orgánica.

Disposición adicional decimonovena. *Derechos de los menores ante Internet.*

En el plazo de un año desde la entrada en vigor de esta ley orgánica, el Gobierno remitirá al Congreso de los Diputados un proyecto de ley dirigido específicamente a garantizar los derechos de los menores ante el impacto de Internet, con el fin de garantizar su seguridad y luchar contra la discriminación y la violencia que sobre los mismos es ejercida mediante las nuevas tecnologías.

Disposición adicional vigésima. *Especialidades del régimen jurídico de la Agencia Española de Protección de Datos.*

1. No será de aplicación a la Agencia Española de Protección de Datos el artículo 50.2.c) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. La Agencia Española de Protección de Datos podrá adherirse a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes prevista en el artículo 85 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Disposición adicional vigésima primera. *Educación digital.*

Las Administraciones educativas darán cumplimiento al mandato contenido en el párrafo segundo del apartado 1 del artículo 83 de esta ley orgánica en el plazo de un año a contar desde la entrada en vigor de la misma.

Disposición adicional vigésima segunda. *Acceso a los archivos públicos y eclesiásticos.*

Las autoridades públicas competentes facilitarán el acceso a los archivos públicos y eclesiásticos en relación con los datos que se soliciten con ocasión de investigaciones policiales o judiciales de personas desaparecidas, debiendo atender las solicitudes con prontitud y diligencia las instituciones o congregaciones religiosas a las que se realicen las peticiones de acceso.

Disposición adicional vigésima tercera. *Modelos de presentación de reclamaciones.*

La Agencia Española de Protección de Datos podrá establecer modelos de presentación de reclamaciones ante la misma en todos los ámbitos en los que ésta tenga competencia, que serán de uso obligatorio para los interesados independientemente de que estén obligados o no a relacionarse electrónicamente con las administraciones públicas.

Los modelos serán publicados en el "Boletín Oficial del Estado" y en la Sede Electrónica de la Agencia Española de Protección de Datos y serán de obligado cumplimiento al mes de su publicación en el "Boletín Oficial del Estado".»

Disposición transitoria primera. *Estatuto de la Agencia Española de Protección de Datos.*

1. El Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, continuará vigente en lo que no se oponga a lo establecido en el Título VIII de esta ley orgánica.

2. Lo dispuesto en los apartados 2, 3 y 5 del artículo 48 y en el artículo 49 de esta ley orgánica se aplicará una vez expire el mandato de quien ostente la condición de Director de la Agencia Española de Protección de Datos a la entrada en vigor de la misma.

Disposición transitoria segunda. *Códigos tipo inscritos en las autoridades de protección de datos conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

Los promotores de los códigos tipo inscritos en el registro de la Agencia Española de Protección de Datos o en las autoridades autonómicas de protección de datos deberán adaptar su contenido a lo dispuesto en el artículo 40 del Reglamento (UE) 2016/679 en el plazo de un año a contar desde la entrada en vigor de esta ley orgánica.

Si, transcurrido dicho plazo, no se hubiera solicitado la aprobación prevista en el artículo 38.4 de esta ley orgánica, se cancelará la inscripción y se comunicará a sus promotores.

Disposición transitoria tercera. *Régimen transitorio de los procedimientos.*

1. Los procedimientos ya iniciados a la entrada en vigor de esta ley orgánica se regirán por la normativa anterior, salvo que esta ley orgánica contenga disposiciones más favorables para el interesado.

2. Lo dispuesto en el apartado anterior será asimismo de aplicación a los procedimientos respecto de los cuales ya se hubieren iniciado las actuaciones previas a las que se refiere la Sección 2.ª del Capítulo III del Título IX del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Disposición transitoria cuarta. *Tratamientos sometidos a la Directiva (UE) 2016/680.*

Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.

Téngase en cuenta que la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, ha sido transpuesta por la Ley Orgánica 7/2021, de 26 de mayo. Ref. BOE-A-2021-8806

Disposición transitoria quinta. *Contratos de encargado del tratamiento.*

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

Disposición transitoria sexta. *Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley orgánica.*

Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:

a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento.

b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

Disposición derogatoria única. *Derogación normativa.*

1. Sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Queda derogado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

3. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición final primera. *Naturaleza de la presente ley.*

La presente ley tiene el carácter de ley orgánica.

No obstante, tienen carácter de ley ordinaria:

– El Título IV,
– el Título VII, salvo los artículos 52 y 53, que tienen carácter orgánico,
– el Título VIII,
– el Título IX,
– los artículos 79, 80, 81, 82, 88, 95, 96 y 97 del Título X,
– las disposiciones adicionales, salvo la disposición adicional segunda y la disposición adicional decimoséptima, que tienen carácter orgánico,
– las disposiciones transitorias,
– y las disposiciones finales, salvo las disposiciones finales primera, segunda, tercera, cuarta, octava, décima y decimosexta, que tienen carácter orgánico.

Disposición final segunda. *Título competencial.*

1. Esta ley orgánica se dicta al amparo del artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

2. El Capítulo I del Título VII, el Título VIII, la disposición adicional cuarta y la disposición transitoria primera sólo serán de aplicación a la Administración General del Estado y a sus organismos públicos.

3. Los artículos 87 a 90 se dictan al amparo de la competencia exclusiva que el artículo 149.1.7.ª y 18.ª de la Constitución reserva al Estado en materia de legislación laboral y bases del régimen estatutario de los funcionarios públicos respectivamente.

4. La disposición adicional quinta y las disposiciones finales séptima y sexta se dictan al amparo de la competencia que el artículo 149.1.6.ª de la Constitución atribuye al Estado en materia de legislación procesal.

5. La disposición adicional tercera se dicta al amparo del artículo 149.1.18.ª de la Constitución.

6. El artículo 96 se dicta al amparo del artículo 149.1.8.ª de la Constitución.

Disposición final tercera. *Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.*

Se modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General que queda redactada como sigue:

Uno. El apartado 3 del artículo treinta y nueve queda redactado como sigue:

«3. Dentro del plazo anterior, cualquier persona podrá formular reclamación dirigida a la Delegación Provincial de la Oficina del Censo Electoral sobre sus datos censales, si bien solo podrán ser tenidas en cuenta las que se refieran a la rectificación de errores en los datos personales, a los cambios de domicilio dentro de una misma circunscripción o a la no inclusión del reclamante en ninguna Sección del Censo de la circunscripción pese a tener derecho a ello. También serán atendidas las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral. No serán tenidas en cuenta para la elección convocada las que reflejen un cambio de residencia de una circunscripción a otra, realizado con posterioridad a la fecha de cierre del censo para cada elección, debiendo ejercer su derecho en la sección correspondiente a su domicilio anterior.»

Dos. Se añade un nuevo artículo cincuenta y ocho bis, con el contenido siguiente:

«Artículo cincuenta y ocho bis. *Utilización de medios tecnológicos y datos personales en las actividades electorales.*

1. **(Anulado)**

2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»

Disposición final cuarta. *Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.*

Se modifica la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, en los siguientes términos:

Uno. Se añade un apartado tercero al artículo 58, con la siguiente redacción:

«Artículo 58.

Tercero. De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por el Consejo General del Poder Judicial.»

Dos. Se añade una letra f) al artículo 66, con la siguiente redacción:

«Artículo 66.

f) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añaden una letra k) al apartado 1 y un nuevo apartado 7 al artículo 74, con la siguiente redacción:

«Artículo 74.

1. […]

k) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.

[…]

7. Corresponde a las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia autorizar, mediante auto, el requerimiento de información por parte de autoridades autonómicas de protección de datos a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Cuatro. Se añade un nuevo apartado 7 al artículo 90:

«7. Corresponde a los Juzgados Centrales de lo Contencioso-administrativo autorizar, mediante auto, el requerimiento de información por parte de la Agencia Española de Protección de Datos y otras autoridades administrativas independientes de ámbito estatal a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Disposición final quinta. *Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad.*

Se añade un nuevo Capítulo II al Título VI de la Ley 14/1986, de 25 de abril, General de Sanidad con el siguiente contenido:

«CAPÍTULO II

Tratamiento de datos de la investigación en salud

Artículo 105 bis.

El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.»

Disposición final sexta. *Modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.*

La Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, se modifica en los siguientes términos:

Uno. Se añade un nuevo apartado 7 al artículo 10:

«7. Conocerán de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.»

Dos. Se añade un nuevo apartado 5 al artículo 11:

«5. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añade un nuevo apartado 4 al artículo 12:

«4. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por el Consejo General del Poder Judicial.»

Cuatro. Se introduce un nuevo artículo 122 ter, con el siguiente tenor:

«Artículo 122 ter. *Procedimiento de autorización judicial de conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos.*

1. El procedimiento para obtener la autorización judicial a que se refiere la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, se iniciará con la solicitud de la autoridad de protección de datos dirigida al Tribunal competente para que se pronuncie acerca de la conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos con el Derecho de la Unión Europea. La solicitud irá acompañada de copia del expediente que se encontrase pendiente de resolución ante la autoridad de protección de datos.

2. Serán partes en el procedimiento, además de la autoridad de protección de datos, quienes lo fueran en el procedimiento tramitado ante ella y, en todo caso, la Comisión Europea.

3. El acuerdo de admisión o inadmisión a trámite del procedimiento confirmará, modificará o levantará la suspensión del procedimiento por posible vulneración de la normativa de protección de datos tramitado ante la autoridad de protección de datos, del que trae causa este procedimiento de autorización judicial.

4. Admitida a trámite la solicitud, el Tribunal competente lo notificará a la autoridad de protección de datos a fin de que dé traslado a quienes interviniesen en el procedimiento tramitado ante la misma para que se personen en el plazo de tres días. Igualmente, se dará traslado a la Comisión Europea a los mismos efectos.

5. Concluido el plazo mencionado en la letra anterior, se dará traslado de la solicitud de autorización a las partes personadas a fin de que en el plazo de diez días aleguen lo que estimen procedente, pudiendo solicitar en ese momento la práctica de las pruebas que estimen necesarias.

6. Transcurrido el período de prueba, si alguna de las partes lo hubiese solicitado y el órgano jurisdiccional lo estimase pertinente, se celebrará una vista. El Tribunal

podrá decidir el alcance de las cuestiones sobre las que las partes deberán centrar sus alegaciones en dicha vista.

7. Finalizados los trámites mencionados en los tres apartados anteriores, el Tribunal competente adoptará en el plazo de diez días una de estas decisiones:

a) Si considerase que la decisión de la Comisión Europea es conforme al Derecho de la Unión Europea, dictará sentencia declarándolo así y denegando la autorización solicitada.

b) En caso de considerar que la decisión es contraria al Derecho de la Unión Europea, dictará auto de planteamiento de cuestión prejudicial de validez de la citada decisión ante el Tribunal de Justicia de la Unión Europea, en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea.

La autorización solamente podrá ser concedida si la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

8. El régimen de recursos será el previsto en esta ley.»

Disposición final séptima. *Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*

Se modifica el artículo 15 bis de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que queda redactado como sigue:

«Artículo 15 bis. *Intervención en procesos de defensa de la competencia y de protección de datos.*

1. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas en el ámbito de sus competencias podrán intervenir en los procesos de defensa de la competencia y de protección de datos, sin tener la condición de parte, por propia iniciativa o a instancia del órgano judicial, mediante la aportación de información o presentación de observaciones escritas sobre cuestiones relativas a la aplicación de los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea o los artículos 1 y 2 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia. Con la venia del correspondiente órgano judicial, podrán presentar también observaciones verbales. A estos efectos, podrán solicitar al órgano jurisdiccional competente que les remita o haga remitir todos los documentos necesarios para realizar una valoración del asunto de que se trate.

La aportación de información no alcanzará a los datos o documentos obtenidos en el ámbito de las circunstancias de aplicación de la exención o reducción del importe de las multas previstas en los artículos 65 y 66 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

2. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas aportarán la información o presentarán las observaciones previstas en el número anterior diez días antes de la celebración del acto del juicio a que se refiere el artículo 433 o dentro del plazo de oposición o impugnación del recurso interpuesto.

3. Lo dispuesto en los anteriores apartados en materia de procedimiento será asimismo de aplicación cuando la Comisión Europea, la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, en el ámbito de sus competencias, consideren precisa su intervención en un proceso que afecte a cuestiones relativas a la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.»

Disposición final octava. *Modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.*

Se incluye una nueva letra l) en el apartado 2 del artículo 46 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, con el contenido siguiente:

«l) La formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.»

Disposición final novena. *Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.*

Se modifica el apartado 3 del artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que pasa a tener el siguiente tenor:

«Artículo 16. *[…]*

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.»

Disposición final décima. *Modificación de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.*

Se incluye una nueva letra l) en el apartado 1 del artículo 2 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, que queda redactado como sigue:

«l) La capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva.»

Disposición final undécima. *Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.*

Se modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en los siguientes términos:

Uno. Se añade un nuevo artículo 6 bis, con la siguiente redacción:

«Artículo 6 bis. *Registro de actividades de tratamiento.*

Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.»

Dos. El apartado 1 del artículo 15 queda redactado como sigue:

«1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.»

Disposición final duodécima. *Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

Se modifican los apartados 2 y 3 del artículo 28 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que pasan a tener la siguiente redacción:

«Artículo 28. *[…]*

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.»

Disposición final decimotercera. *Modificación del texto refundido de la Ley del Estatuto de los Trabajadores.*

Se añade un nuevo artículo 20 bis al texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, con el siguiente contenido:

> **«Artículo 20 bis.** *Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.*
>
> Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimocuarta. *Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.*

Se añade una nueva letra j bis) en el artículo 14 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, que quedará redactada como sigue:

> «j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimoquinta. *Desarrollo normativo.*

Se habilita al Gobierno para desarrollar lo dispuesto en los artículos 3.2, 38.6, 45.2, 63.3, 96.3 y disposición adicional sexta, en los términos establecidos en ellos.

Disposición final decimosexta. *Entrada en vigor.*

La presente ley orgánica entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

§ 3

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 298, de 14 de diciembre de 1999
Última modificación: 6 de diciembre de 2018
Referencia: BOE-A-1999-23750

Norma derogada, con efectos de 7 de diciembre de 2018, sin perjuicio de lo previsto en la disposición adicional 14 de la Ley Orgánica 3/2018, de 5 de diciembre, según establece su disposición derogatoria única.1. Ref. BOE-A-2018-16673

[. . .]

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

[. . .]

Artículo 22. *Ficheros de las Fuerzas y Cuerpos de Seguridad.*

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. *Excepciones a los derechos de acceso, rectificación y cancelación.*

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. *Otras excepciones a los derechos de los afectados.*

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado **impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas** o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales **o administrativas**.

> Téngase en cuenta que se declara la inconstitucionalidad y nulidad de los incisos destacados del apartado 1 por Sentencia del TC 292/2000, de 30 de noviembre. Ref. BOE-T-2001-332

2. **(Anulado)**

[. . .]

§ 4

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales

Jefatura del Estado
«BOE» núm. 126, de 27 de mayo de 2021
Última modificación: 29 de julio de 2022
Referencia: BOE-A-2021-8806

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica:

PREÁMBULO

I

La Unión Europea es un espacio en el que los estándares y las garantías de protección de los derechos de las personas físicas a la protección de los datos personales se encuentran en la vanguardia internacional y constituyen un referente mundial. El rápido desarrollo tecnológico, especialmente de Internet, así como la creciente globalización de la economía mundial y europea han hecho imprescindible abordar la reforma del marco jurídico de la protección de datos, al objeto de consolidar e incluso mejorar este elevado nivel de protección a través de la creación de un marco legislativo nuevo, adaptado a la realidad cambiante, al tiempo que sólido, coherente e integral. En definitiva, un entorno normativo para un mundo globalizado y digital.

En este sentido, la Comunicación de la Comisión Europea «Un enfoque global de la protección de los datos personales en la Unión Europea», de 4 de noviembre de 2010, precedida de un intenso periodo de consultas durante más de dos años con los Estados miembros, el público en general, así como con los distintos sectores afectados, sentó las bases de lo que sería esta nueva perspectiva normativa.

El marco normativo resultante consta, principalmente, de dos instrumentos: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), que sustituye a una norma vigente

desde hacía más de veinte años, y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

En nuestro ordenamiento jurídico, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, adaptó el Reglamento General de Protección de Datos, en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.

II

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, objeto de transposición por esta Ley Orgánica, deroga la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, que había sido superada por varias razones.

En primer lugar, se trataba de una norma previa al Tratado de Lisboa que requería de su oportuna adaptación a los nuevos Tratados, en particular, al artículo 16 del Tratado de Funcionamiento de la Unión Europea, que exige que el Consejo y el Parlamento Europeo, a través del procedimiento legislativo ordinario, regulen la protección de los datos personales.

En segundo término, la decisión marco se aprobó conforme a la estructura de pilares de la Unión Europea, previa al Tratado de Lisboa, por lo que contaba con un ámbito de aplicación limitado exclusivamente al tratamiento de datos personales de carácter transfronterizo entre los Estados miembros, sin alcanzar, por tanto, a los tratamientos de carácter estrictamente nacional.

Asimismo, otorgaba una amplísima capacidad de maniobra a los Estados miembros, sin asegurar un nivel mínimo de armonización deseable en determinados ámbitos, como el reconocimiento en todos los Estados del derecho de acceso de los interesados a sus propios datos, el principio del tratamiento de los datos para fines determinados o las condiciones para las transferencias internacionales.

En definitiva, la fragmentación y complejidad de la regulación en este campo perjudicaba la necesaria confianza entre los actores de la cooperación policial y judicial penal en Europa, quienes mostraban recelos a compartir información, entre otros motivos, por la ausencia de una mínima armonización en cuanto a la protección de los datos de carácter personal; unos datos que resultan esenciales en el terreno de la cooperación operativa.

III

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, subsana estas deficiencias, ampliando su ámbito de aplicación al tratamiento nacional de los datos personales en el espacio de la cooperación policial y judicial penal. Toda vez que cubre otras carencias de la normativa europea anterior, dado que incluye la regulación de los datos genéticos –que reclamaba el Tribunal Europeo de Derechos Humanos-, así como la distinción entre los datos personales según su grado de exactitud y fiabilidad, o la diferenciación entre distintas categorías de interesados.

Resulta pertinente poner de relieve que la citada directiva que transpone esta Ley Orgánica se aprobó como respuesta a las crecientes amenazas para la seguridad en el contexto nacional e internacional, que tienen, en numerosos casos, un componente transfronterizo. Por esta razón, la cooperación internacional y la transmisión de información de carácter personal entre los servicios policiales y judiciales de los países implicados se convierten en un objetivo ineludible. En efecto, los atentados terroristas de Nueva York en 2001 supusieron un punto de inflexión en la necesidad de reforzar la cooperación judicial y policial en la lucha contra el terrorismo, como volvería a ponerse de manifiesto con ocasión de los atentados de Bruselas y Niza en 2016.

La cooperación encaminada a compartir a tiempo la información operativa precisa se erige en un requisito de eficacia en la prevención y lucha contra este tipo de amenazas. Todo

ello, teniendo en cuenta el estado de la técnica, que permite, en la actualidad, tratamientos de datos a gran escala en el ámbito de la seguridad.

Este intercambio de información debe realizarse, en todo caso, de manera que se garanticen los principios democráticos y la seguridad de las personas a lo largo de las fases del tratamiento.

En consecuencia, esta Ley Orgánica asume la finalidad de lograr un elevado nivel de protección de los derechos de la ciudadanía, en general, y de sus datos personales, en particular, que resulte homologable al del resto de los Estados miembros de la Unión Europea, incorporando y concretando las reglas que establece la directiva.

En este sentido, la Constitución española fue precursora del reconocimiento y la defensa del derecho fundamental a la protección de datos personales. Así, el artículo 18.4 de nuestra norma fundamental dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de la ciudadanía y el pleno ejercicio de sus derechos. El Tribunal Constitucional, en reiterada jurisprudencia, entiende la protección de datos como un derecho fundamental que garantiza a toda persona la capacidad de controlar el uso y destino de sus datos, con el propósito de evitar el tráfico ilícito o lesivo de los mismos o una utilización para fines distintos de los que justificaron su obtención.

Por todo ello, la transposición de esta directiva por los Estados miembros supone el establecimiento de un marco jurídico consistente, que proporciona la seguridad jurídica necesaria para facilitar la cooperación policial y judicial penal y, por tanto, una mayor eficacia en el desempeño de sus funciones por las Fuerzas y Cuerpos de Seguridad y de nuestro sistema judicial penal en su conjunto, incluido el penitenciario.

IV

Esta Ley Orgánica consta de sesenta y cinco artículos estructurados en ocho capítulos, cinco disposiciones adicionales, una disposición transitoria, una disposición derogatoria y doce disposiciones finales.

El capítulo I, relativo a las disposiciones generales, define el objeto de la Ley Orgánica, entendiéndose como la regulación del tratamiento de los datos personales para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluida la protección y de prevención frente a las amenazas contra la seguridad pública, cuando dicho tratamiento se lleve a cabo por los órganos que, a efectos de esta Ley Orgánica, tengan la consideración de autoridades competentes.

La finalidad principal es que los datos sean tratados por estas autoridades competentes de manera que se cumplan los fines prevenidos a la par que establecer los mayores estándares de protección de los derechos fundamentales y las libertades de los ciudadanos, de forma que se cumpla lo dispuesto en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, así como en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea y el artículo 18.4 de la Constitución.

Asimismo, en correspondencia con lo que dispone el artículo 22.6 de la Ley Orgánica 3/2018, de 5 de diciembre, cuando el tratamiento de los datos personales se realice para alguno de los fines establecidos en esta Ley Orgánica y proceda de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad, o bien se lleve a cabo por los órganos competentes para la vigilancia y control en los centros penitenciarios o para el control, regulación, vigilancia y disciplina del tráfico, dichos tratamientos se regularán por las disposiciones de esta Ley Orgánica complementándose, en lo que no resulte contrario a su contenido, con la normativa vigente que regula estos ámbitos. De este modo, se establece un nuevo sistema que gira en torno a las obligaciones de los responsables del tratamiento y a las distintas misiones que se les asignan.

Aunque se deben excluir con carácter general, se incluyen igualmente algunas previsiones específicas para el tratamiento de los datos de personas fallecidas a similitud de lo que se dispone en la precitada Ley Orgánica 3/2018, de 5 de diciembre.

Las autoridades competentes, a efectos de esta Ley Orgánica, se definen como autoridades públicas con competencias legalmente encomendadas para la consecución de los fines específicos incluidos en el ámbito de aplicación. En concreto, se determina que serán autoridades competentes: las Fuerzas y Cuerpos de Seguridad; las autoridades

judiciales del orden jurisdiccional penal y el Ministerio Fiscal; las Administraciones Penitenciarias; la Dirección Adjunta de Vigilancia Aduanera; el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias; y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo. Todo ello, sin perjuicio de que los tratamientos que se lleven a cabo por los órganos jurisdiccionales se rijan por lo dispuesto en esta Ley Orgánica, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales penales.

Se excluyen expresamente del ámbito de aplicación ciertos tratamientos, como los realizados por las autoridades competentes para fines distintos de los cubiertos por la Ley Orgánica; los llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito del capítulo II del título V del Tratado de la Unión Europea, en relación a la Política Exterior y de Seguridad Común; los derivados de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión Europea; y los sometidos a la normativa sobre materias clasificadas. Entre estos últimos se mencionan expresamente como incluidos los tratamientos relativos a la Defensa Nacional.

El capítulo II se refiere a los principios de protección de datos cuya garantía corresponde al responsable del tratamiento. Estos principios se regulan en términos similares a lo establecido en el Reglamento General de Protección de Datos, con algunas especialidades propias del ámbito de esta Ley Orgánica.

Se incluye un deber de colaboración con las autoridades competentes, según el cual, salvo que legalmente sea exigible una autorización judicial, las Administraciones Públicas o cualquier persona física o jurídica deberá proporcionar a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial la información necesaria para la investigación o enjuiciamiento de infracciones penales o la ejecución de las penas y la información necesaria para la protección y prevención frente a un peligro real y grave para la seguridad pública. Todo ello, con la obligación de no informar al interesado de dichos tratamientos ulteriores. Esta última precisión resulta fundamental para evitar que la puesta de la información a disposición del interesado pueda poner en peligro los fines que, de acuerdo con la directiva y esta Ley Orgánica, justifican el tratamiento de los datos.

Se regulan, también, los plazos de conservación y de revisión de los datos de carácter personal tratados, siendo relevante el establecimiento de un plazo máximo de conservación de los datos con carácter general y la implantación de un sistema que permite al responsable revisar, en el plazo que el mismo establezca dentro del margen legal, la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de sus actividades de tratamiento. El responsable deberá, en sus tratamientos, distinguir los datos que correspondan a las diversas categorías de interesados, tales como los sospechosos, los condenados o los sancionados, las víctimas o los terceros involucrados, así como diferenciar, en la medida de lo posible, si los datos que trata son datos basados en hechos o en apreciaciones.

Se exigen igualmente ciertas condiciones que determinan la licitud de todo tratamiento de datos de carácter personal, esto es, que sean tratados por las autoridades competentes; que resulten necesarios para los fines de esta Ley Orgánica y que, en caso necesario y en cada ámbito particular, se especifiquen las especialidades por una norma con rango de ley que incluya unos contenidos mínimos.

En el supuesto de transmisión de datos sujetos a condiciones específicas de tratamiento, dichas condiciones deberán ser respetadas por el destinatario de los mismos, en especial, la prohibición de transmitirlos o de utilizarlos para fines distintos para los que fueron transmitidos.

De igual modo, se exige que el tratamiento de categorías especiales de datos, como son los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical o los genéticos o biométricos, sólo pueda tener lugar cuando sea estrictamente necesario y se cumplan ciertas condiciones.

Los datos biométricos (como las huellas dactilares o la imagen facial) sólo se consideran incluidos en esta categoría especial cuando su tratamiento está dirigido a identificar de manera unívoca a una persona física. Esta necesidad de identificación en las actuaciones amparadas legalmente se lleva a cabo, con frecuencia, por las distintas autoridades competentes. El propósito es singularizar los autores o partícipes de infracciones penales,

así como poder reconocer si son las personas que se supone o se busca, y de esta forma, atribuir o exonerar, sin género de dudas, la participación en determinados hechos, gracias a posibles indicios o vestigios biométricos.

Habida cuenta de la vertiginosa evolución tecnológica y los medios electrónicos de los que se dispone, se incluye la habilitación legal que facilite una respuesta rápida y adecuada en el uso de estos datos, con el objetivo final de garantizar y proteger los derechos de los interesados y de la ciudadanía en general.

Se prohíbe, igualmente, la adopción de decisiones individuales automatizadas, incluida la elaboración de perfiles en este ámbito, salvo que esté autorizado por una norma con rango de ley del ordenamiento jurídico español o europeo.

El capítulo III, se divide en dos secciones y aborda los derechos de las personas. Regula una serie de condiciones generales del ejercicio de los derechos, tales como la obligación exigible al responsable de facilitar la información correspondiente a los derechos del interesado de forma concisa, con un lenguaje claro y sencillo y de manera gratuita. Se establece la información que debe ponerse a disposición del interesado, siendo algunos datos obligatorios, en todo caso, y otros en casos concretos.

Se reconocen los derechos de acceso, rectificación, supresión y limitación del tratamiento. En virtud de tales derechos se faculta al interesado a conocer si se están tratando o no sus datos y, en caso afirmativo, acceder a cierta información sobre el tratamiento; a obtener la rectificación de sus datos si estos resultaran inexactos; a suprimirlos cuando fueran contrarios a lo dispuesto en los artículos 6, 11 o 13, o cuando así lo requiera una obligación legal exigible al responsable; y a limitar el tratamiento, cuando el interesado ponga en duda la exactitud de los datos o estos datos deban conservarse únicamente a efectos probatorios.

Estos derechos podrán ser ejercidos por el interesado directamente o, en determinados casos, a través de la autoridad de protección de datos.

Dispone esta Ley Orgánica que estos derechos pueden ser restringidos por ciertas causas tasadas, como cuando sea necesario para evitar que se obstaculice una investigación o se ponga en peligro la seguridad pública o la seguridad nacional.

Se establece, en su sección segunda, un régimen especial de derechos de los interesados en el marco de investigaciones y procesos penales.

El capítulo IV recoge las obligaciones y responsabilidades de los responsables y encargados de protección de datos, las medidas de seguridad y la figura del delegado de protección de datos, a lo largo de tres secciones. El responsable del tratamiento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicará las medidas técnicas y organizativas apropiadas.

El encargado del tratamiento llevará a cabo sus funciones por cuenta del responsable, debiendo ofrecer garantías para aplicar medidas técnicas y organizativas apropiadas.

Todo responsable y encargado del tratamiento deberá conservar un registro de actividades de tratamiento, con datos identificativos, tales como los datos de contacto del responsable, los fines o las categorías de interesados, y un registro de operaciones, pieza angular de este sistema e instrumento básico para acreditar el cumplimiento de varios de los principios de tratamiento, que comprenderá la recogida, la alteración, las consultas y las transferencias de los datos personales entre otras operaciones. Asimismo, están obligados a cooperar con la autoridad de protección de datos, en el marco de la legislación vigente.

Se establecen ciertas obligaciones que responden a un nuevo modelo de responsabilidad activa que exige una valoración previa del riesgo que pudiera generar el tratamiento de los datos de carácter personal para los interesados, para, a partir de dicha valoración, adoptar las medidas que procedan.

Se presta una atención detallada a la seguridad del tratamiento, regulándose alguna de las medidas de seguridad que se aplicarán, si bien solo se dispone como obligatoria la puesta en marcha del citado registro de operaciones como medida técnica y organizativa, siendo las demás las que el responsable determine como las más adecuadas para lograr el control que se le solicita en virtud del tipo de tratamiento que se esté llevando a cabo y del nivel de riesgo que se estime, tras el correspondiente análisis. Se impone, asimismo, el deber de notificación a la autoridad de protección de datos de cualquier violación de la

seguridad que, con carácter general, deberá ser notificada al interesado, salvo en supuestos expresamente previstos en la ley.

El delegado de protección de datos se configura como el órgano o figura de asesoramiento y supervisión de los responsables de protección de datos, que podrá ser único para varias autoridades competentes y cuya designación será obligatoria salvo en relación con los tratamientos de datos con fines jurisdiccionales. En el caso de que se dispongan tratamientos que queden bajo distintos ámbitos de aplicación, con el fin de evitar disfunciones en las organizaciones de las autoridades competentes, se establece que la figura del delegado de protección de datos será única para todos ellos.

El capítulo V regula las transferencias de datos personales realizadas por las autoridades competentes españolas a un Estado que no sea miembro de la Unión Europea o a una organización internacional, incluidas las transferencias ulteriores a otro Estado que no pertenezca a la Unión Europea u otra organización internacional y se establecen las condiciones que deberán cumplirse para que estas sean lícitas.

Así, con el fin de garantizar que no se menoscabe el nivel de protección de las personas físicas previsto en esta Ley Orgánica, la transferencia respetará ciertas condiciones previstas en la misma. De este modo, sólo deben realizarse cuando sean necesarias para los fines de esta Ley Orgánica y cuando el responsable del tratamiento en el tercer país u organización internacional sea autoridad competente en relación a dichos fines.

Asimismo, cuando el dato se transfiere a un tercer país o a una organización internacional, la autoridad competente del Estado miembro en el que se obtuvo el dato, debe autorizar previamente esta transferencia y las ulteriores que puedan tener lugar a otro tercer país o a una organización internacional. En cuanto al tercer país u organización internacional destinatario de la trasferencia, deberá ser objeto de evaluación por la Comisión Europea a la vista de su nivel de protección de datos o, en caso de ausencia de decisión, debe entenderse por el responsable del tratamiento que ofrece garantías adecuadas. Sólo por las causas excepcionales previstas en esta Ley Orgánica se podrán autorizar transferencias fuera de estos supuestos. Este capítulo finaliza con la regulación de la transferencia internacional de datos personales a destinatarios que, no siendo autoridades competentes, están establecidos en terceros países.

El capítulo VI, relativo a las autoridades de protección de datos, dispone que dichas autoridades sean la Agencia Española de Protección de Datos y las Agencias Autonómicas de Protección de Datos, en sus respectivos ámbitos competenciales. Asimismo, la Ley Orgánica recoge sus potestades, funciones y la asistencia entre autoridades de protección de datos de los Estados miembros. Se remite en lo restante a la normativa que les resulte de aplicación.

El capítulo VII prevé que los procedimientos de reclamación que se planteen ante las autoridades de protección de datos se rijan por lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, o, en su caso, por la normativa reguladora de la autoridad de protección de datos correspondiente. Se refiere a aquellos supuestos en que los responsables o encargados del tratamiento, o de la autoridad de protección de datos, en su caso, incumplan esta Ley Orgánica y generen un daño o lesión en los bienes o derechos del interesado.

Este capítulo, además, aborda la responsabilidad de los responsables o encargados del tratamiento o de la autoridad de protección de datos, en su caso, cuando incumplan esta Ley Orgánica y se genere un daño o lesión en los bienes o derechos de un interesado. De igual modo, se detalla la forma de ejercer el derecho a la tutela judicial efectiva ante la jurisdicción contencioso-administrativa contra las decisiones de una autoridad de protección de datos que puedan entenderse que conciernen a los interesados.

Finalmente, el capítulo VIII regula el régimen sancionador específico aplicable ante incumplimientos de las obligaciones previstas en esta Ley Orgánica. Se definen los sujetos sobre los que recaerá la responsabilidad por las infracciones cometidas. Se determinan las reglas del concurso de normas para resolver los casos en los que un hecho pueda ser calificado con arreglo a dos o más de ellas, al tiempo que se tipifican las infracciones, que, en función de su gravedad, podrán ser leves, graves o muy graves. Por último, se establecen las sanciones que se pueden imponer, y se fijan los plazos de prescripción tanto de las infracciones como de las sanciones y de caducidad.

Las disposiciones adicionales se refieren a regímenes específicos, al intercambio de datos dentro de la Unión Europea, a los acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, y a los tratamientos que se efectúen en relación con los ficheros y al Registro de Población de las Administraciones Públicas.

Las disposiciones finales introducen las modificaciones necesarias en la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria, para adecuarla a las previsiones de esta Ley Orgánica en relación con los tratamientos para ejecución de la pena; en la Ley 50/1981, de 30 de diciembre; en la Ley Orgánica 6/1985, de 1 de julio; en la Ley Orgánica 3/2018, de 5 de diciembre; en la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves en correspondencia con determinadas obligaciones de los operadores; en la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte; en la Ley 5/2014, de 4 de abril, de Seguridad Privada para adecuar, en ambos casos, los plazos de caducidad de los expedientes sancionadores; y en el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 6/2015, de 30 de octubre, para dar soporte legal específico a las matriculaciones por razones de Seguridad Nacional.

En la elaboración de esta Ley Orgánica se han observado los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, exigidos por el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En primer lugar, se trata de una norma necesaria, dado que la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, exige una ley de carácter orgánico, al afectar la norma comunitaria a un derecho fundamental reconocido en el artículo 18 de la Constitución y por imperativo del artículo 81 de la misma. En este sentido, el artículo 18.4 de la Constitución dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de la ciudadanía y el pleno ejercicio de sus derechos.

Esta Ley Orgánica, además, incorpora a nuestro ordenamiento interno los instrumentos que permitirán una eficaz protección de los datos de las personas físicas frente a su tratamiento por parte de las autoridades competentes con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

Por lo que respecta al principio de seguridad jurídica, en razón de la materia objeto de regulación, la transposición de la directiva se realiza mediante una Ley Orgánica, cuya tramitación e integración en el ordenamiento jurídico goza de las garantías que amparan las normas de esta naturaleza.

En cuanto al principio de proporcionalidad, esta Ley Orgánica contempla un importante número de garantías orientadas a que el tratamiento de datos personales sea proporcional, oportuno, mínimo y suficiente para el cumplimiento de los fines que se persiguen. En particular, su tratamiento se sujeta a los principios que rigen el tratamiento de datos personales, por lo que se exige que no sean tratados para otros fines distintos de los establecidos en la norma, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por nuestro Derecho interno. Cuando los datos personales sean tratados para otros fines que no sean los de la prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública, se aplicará el Reglamento General de Protección de Datos, a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión Europea.

Se cumple, también, el principio de transparencia, puesto que esta norma ha sido sometida a los correspondientes trámites de participación pública, esto es, el de consulta pública previa y el de audiencia e información pública.

En la tramitación de esta Ley Orgánica, además de los diversos Ministerios concernidos por razón de la materia, han emitido informe la Agencia Española de Protección de Datos; la Agencia Vasca de Protección de Datos; la Autoridad Catalana de Protección de Datos; el

Consejo Fiscal; el Consejo General del Poder Judicial; los Departamentos de Seguridad Pública del Gobierno Vasco y de Interior de la Generalidad de Cataluña; y finalmente el Consejo de Estado. Se trata, por tanto, de un texto en el cual se han incorporado las consideraciones de órganos tan relevantes como los expuestos.

Por último, esta Ley Orgánica se dicta al amparo de las reglas 1.ª, 6.ª, 18.ª y 29.ª del artículo 149.1 de la Constitución, que atribuyen al Estado las competencias exclusivas, respectivamente, para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales; sobre legislación penal, penitenciaria y procesal; respecto a las bases del régimen jurídico de las Administraciones Públicas, el procedimiento administrativo común y en relación al sistema de responsabilidad de todas las Administraciones públicas; y en materia de seguridad pública.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Esta Ley Orgánica tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Artículo 2. *Ámbito de aplicación.*

1. Será de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, realizado por las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

2. El tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de las actuaciones o procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, en el ámbito del artículo 1, se regirá por lo dispuesto en la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, las leyes procesales que le sean aplicables y, en su caso, por la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal. Las autoridades de protección de datos a las que se refiere el capítulo VI no serán competentes para controlar estas operaciones de tratamiento.

3. Quedan fuera del ámbito de aplicación de esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los realizados por las autoridades competentes para fines distintos de los previstos en el artículo 1, incluidos los fines de archivo por razones de interés público, investigación científica e histórica o estadísticos. Estos tratamientos se someterán plenamente a lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

b) Los llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito de aplicación del capítulo II del título V del Tratado de la Unión Europea.

c) Los tratamientos que afecten a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea.

d) Los sometidos a la normativa sobre materias clasificadas, entre los que se encuentran los tratamientos relativos a la Defensa Nacional.

e) Los tratamientos realizados en las acciones civiles y procedimientos administrativos o de cualquier índole vinculados con los procesos penales que no tengan como objetivo directo ninguno de los fines del artículo 1.

4. Esta Ley Orgánica no se aplicará a los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo siguiente.

Artículo 3. *Datos de personas fallecidas.*

1. Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso, rectificación o supresión de los datos de aquel. Estos derechos se regularán de acuerdo con lo dispuesto en esta Ley Orgánica.

2. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona interesada.

3. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el apartado anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Artículo 4. *Autoridades competentes.*

1. Será autoridad competente, a los efectos de esta Ley Orgánica, toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos en el artículo 1.

En particular, tendrán esa consideración, en el ámbito de sus respectivas competencias, las siguientes autoridades:

a) Las Fuerzas y Cuerpos de Seguridad.

b) Las Administraciones Penitenciarias.

c) La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria.

d) El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

e) La Comisión de Vigilancia de Actividades de Financiación del Terrorismo.

2. También tendrán consideración de autoridades competentes las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

Artículo 5. *Definiciones.*

A efectos de esta Ley Orgánica se entenderá por:

a) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

b) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

c) «limitación del tratamiento»: el marcado de los datos personales conservados con el fin de limitar su tratamiento en el futuro;

d) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

e) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

f) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o dispersado de forma funcional o geográfica;

g) «responsable del tratamiento» o «responsable»: la autoridad competente que sola o conjuntamente con otras, determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión Europea o por la legislación española, dichas normas podrán designar al responsable del tratamiento, o bien los criterios para su nombramiento.

h) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

i) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerará destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con la legislación española o de la Unión Europea; el tratamiento de tales datos por las citadas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

j) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita, o la comunicación o acceso no autorizados a datos personales transmitidos, conservados o tratados de otra forma;

k) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de la persona física de que se trate;

l) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

m) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

n) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

CAPÍTULO II

Principios, licitud del tratamiento y videovigilancia

Sección 1.ª Principios y licitud del tratamiento

Artículo 6. *Principios relativos al tratamiento de datos personales.*

1. Los datos personales serán:

a) Tratados de manera lícita y leal.

b) Recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines.

c) Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados.

d) Exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen, sin dilación indebida, los datos personales que sean inexactos con respecto a los fines para los que son tratados.

e) Conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados.

f) Tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Para ello, se utilizarán las medidas técnicas u organizativas adecuadas.

2. Los datos personales recogidos por las autoridades competentes no serán tratados para otros fines distintos de los establecidos en el artículo 1, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por la legislación española. Cuando los datos personales sean tratados para otros fines, se aplicará el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión Europea.

3. Los datos personales podrán ser tratados por el mismo responsable o por otro, para fines establecidos en el artículo 1 distintos de aquel para el que hayan sido recogidos, en la medida en que concurran cumulativamente las dos circunstancias siguientes:

a) Que el responsable del tratamiento sea competente para tratar los datos para ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española.

b) Que el tratamiento sea necesario y proporcionado para la consecución de ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española.

4. El tratamiento por el mismo responsable o por otro podrá incluir el archivo por razones de interés público, y el uso científico, estadístico o histórico para los fines establecidos en el artículo 1, con sujeción a las garantías adecuadas para los derechos y libertades de los interesados.

5. El responsable del tratamiento deberá garantizar y estar en condiciones de demostrar el cumplimiento de lo establecido en este artículo.

Artículo 7. *Deber de colaboración.*

1. Las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas. La petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que le encomienda el artículo 549.1 de la Ley Orgánica 6/1985, de 1 de julio y deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal.

La comunicación de datos, informes, antecedentes y justificantes por la Administración Tributaria, la Administración de la Seguridad Social y la Inspección de Trabajo y Seguridad Social, se efectuará de acuerdo con su legislación respectiva.

2. En los restantes casos, las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública. La petición de la autoridad competente deberá ser concreta y específica y contener la motivación que acredite su relación con los indicados supuestos.

3. No será de aplicación lo dispuesto en los apartados anteriores cuando legalmente sea exigible la autorización judicial para recabar los datos necesarios para el cumplimiento de los fines del artículo 1.

4. En los supuestos contemplados en los apartados anteriores, el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber

facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora.

Con el mismo propósito, los sujetos a los que el ordenamiento jurídico imponga un deber específico de colaboración con las autoridades competentes para el cumplimiento de los fines establecidos en el artículo 1, no informarán al interesado de la transmisión de sus datos a dichas autoridades, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, en cumplimiento de sus obligaciones específicas.

Artículo 8. *Plazos de conservación y revisión.*

1. El responsable del tratamiento determinará que la conservación de los datos personales tenga lugar sólo durante el tiempo necesario para cumplir con los fines previstos en el artículo 1.

2. El responsable del tratamiento deberá revisar la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento bajo su responsabilidad, como máximo cada tres años, atendiendo especialmente en cada revisión a la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal. Si es posible, se hará mediante el tratamiento automatizado apropiado.

3. Con carácter general, el plazo máximo para la supresión de los datos será de veinte años, salvo que concurran factores como la existencia de investigaciones abiertas o delitos que no hayan prescrito, la no conclusión de la ejecución de la pena, reincidencia, necesidad de protección de las víctimas u otras circunstancias motivadas que hagan necesario el tratamiento de los datos para el cumplimiento de los fines del artículo 1.

Artículo 9. *Distinción entre categorías de interesados.*

El responsable del tratamiento, en la medida de lo posible, establecerá entre los datos personales de las distintas categorías de interesados, distinciones tales como:

a) Personas respecto de las cuales existan motivos fundados para presumir que hayan cometido, puedan cometer o colaborar en la comisión de una infracción penal.

b) Personas condenadas o sancionadas por una infracción penal.

c) Víctimas o afectados por una infracción penal o que puedan serlo.

d) Terceros involucrados en una infracción penal como son: personas que puedan ser citadas a testificar en investigaciones relacionadas con infracciones o procesos penales ulteriores, personas que puedan facilitar información sobre dichas infracciones, o personas de contacto o asociados de una de las personas mencionadas en las letras a) y b).

Lo anterior no debe impedir la aplicación del derecho a la presunción de inocencia tal como lo garantiza el artículo 24 de la Constitución.

Artículo 10. *Verificación de la calidad de los datos personales.*

1. El responsable del tratamiento, en la medida de lo posible, establecerá una distinción entre los datos personales basados en hechos y los basados en apreciaciones personales.

2. Las autoridades competentes adoptarán todas las medidas razonables para garantizar que los datos personales que sean inexactos, incompletos o no estén actualizados, no se transmitan ni se pongan a disposición de terceros. En toda transmisión de datos se trasladará al mismo tiempo la valoración de su calidad, exactitud y actualización.

En la medida de lo posible, en todas las transmisiones de datos personales se añadirá la información necesaria para que la autoridad competente receptora pueda valorar hasta qué punto son exactos, completos y fiables, y en qué medida están actualizados. Igualmente, la autoridad competente transmisora, en la medida en que sea factible, controlará la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de terceros.

3. Si se observara que los datos personales transmitidos son incorrectos o que se han transmitido ilegalmente, estas circunstancias se pondrán en conocimiento del destinatario sin dilación indebida. En tal caso, los datos deberán rectificarse o suprimirse, o el tratamiento deberá limitarse de conformidad con lo previsto en el artículo 23.

Artículo 11. *Licitud del tratamiento.*

1. El tratamiento sólo será lícito en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones.

2. Cualquier ley que regule tratamientos de datos personales para los fines incluidos dentro del ámbito de aplicación de esta Ley Orgánica deberá indicar, al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento.

Artículo 12. *Condiciones específicas de tratamiento.*

1. Cuando el Derecho de la Unión Europea o la legislación española prevea condiciones específicas aplicables al tratamiento, la autoridad competente transmitente deberá informar al destinatario al que se transmitan los datos, de dichas condiciones y de la obligación de respetarlas.

2. Las condiciones específicas de tratamiento podrán ser, entre otras, la prohibición de transmisión de datos o de su utilización para fines distintos para los que fueron transmitidos o, en caso de limitación del derecho a la información, la prohibición de dar información al interesado sin la autorización previa de la autoridad transmisora.

3. La autoridad competente transmitente no aplicará a los destinatarios de otros Estados miembros de la Unión Europea o de organismos, agencias y órganos establecidos en virtud de los capítulos 4 y 5 del título V de la tercera parte del Tratado de Funcionamiento de la Unión Europea, condiciones distintas de las aplicables a las transmisiones de datos similares dentro de España.

Artículo 13. *Tratamiento de categorías especiales de datos personales.*

1. El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física, sólo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:

a) Se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea.

b) Resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física.

c) Dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

2. Las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

3. Los datos de los menores de edad y de las personas con capacidad modificada judicialmente o que estén incursas en procesos de dicha naturaleza, se tratarán garantizando el interés superior de los mismos y con el nivel de seguridad adecuado.

Artículo 14. *Mecanismo de decisión individual automatizado.*

1. Están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada.

2. Las decisiones a las que se refiere el apartado anterior no se basarán en las categorías especiales de datos personales contempladas en el artículo 13, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

3. Queda prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales establecidas en el artículo 13.

Sección 2.ª Tratamiento de datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de Seguridad

Artículo 15. *Sistemas de grabación de imágenes y sonido por las Fuerzas y Cuerpos de Seguridad.*

1. La captación, reproducción y tratamiento de datos personales por las Fuerzas y Cuerpos de Seguridad en los términos previstos en esta Ley Orgánica, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. En la instalación de sistemas de grabación de imágenes y sonidos se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones propias; asegurar la protección de edificios e instalaciones públicas y de sus accesos que estén bajo custodia; salvaguardar y proteger las instalaciones útiles para la seguridad nacional y prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública.

Artículo 16. *Instalación de sistemas fijos.*

1. En las vías o lugares públicos donde se instalen videocámaras fijas, el responsable del tratamiento deberá realizar una valoración del citado principio de proporcionalidad en su doble versión de idoneidad e intervención mínima. Asimismo, deberá llevar a cabo un análisis de los riesgos o una evaluación de impacto de protección de datos relativo al tratamiento que se pretenda realizar, en función del nivel de perjuicio que se pueda derivar para la ciudadanía y de la finalidad perseguida.

Se entenderá por videocámara fija aquella anclada a un soporte fijo o fachada, aunque el sistema de grabación se pueda mover en cualquier dirección.

2. Esta disposición se aplicará asimismo cuando las Fuerzas y Cuerpos de Seguridad utilicen instalaciones fijas de videocámaras de las que no sean titulares y exista, por su parte, un control y dirección efectiva del proceso completo de tratamiento.

3. Estas instalaciones fijas de videocámaras no estarán sujetas al control preventivo de las entidades locales previsto en su legislación reguladora básica, ni al ejercicio de las competencias de las diferentes Administraciones públicas, sin perjuicio de que deban respetar los principios de la legislación vigente en cada ámbito material de la actuación administrativa.

4. Los propietarios y, en su caso, los titulares de derechos reales sobre los bienes afectados por estas instalaciones, o quienes los posean por cualquier título, están obligados a facilitar y permitir su instalación y mantenimiento, sin perjuicio de las indemnizaciones que procedan.

5. Los ciudadanos serán informados de manera clara y permanente de la existencia de estas videocámaras fijas, sin especificar su emplazamiento, así como de la autoridad responsable del tratamiento ante la que poder ejercer sus derechos.

Artículo 17. *Dispositivos móviles.*

1. Podrán utilizarse dispositivos de toma de imágenes y sonido de carácter móvil para el mejor cumplimiento de los fines previstos en esta Ley Orgánica, conforme a las competencias específicas de las Fuerzas y Cuerpos de Seguridad. La toma de imagen y

sonido, que ha de ser conjunta, queda supeditada, en todo caso, a la concurrencia de un peligro o evento concreto. El uso de los dispositivos móviles deberá estar autorizado por la persona titular de la Delegación o Subdelegación del Gobierno, quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización de dichos dispositivos a los principios de tratamiento y al de proporcionalidad.

En el caso de los Cuerpos de Policía propios de las Comunidades Autónomas que tengan y ejerzan competencias asumidas para la protección de las personas y bienes y para el mantenimiento del orden público, serán sus órganos correspondientes los que autorizarán este tipo de actuaciones para sus fuerzas policiales, así como para las dependientes de las Corporaciones locales radicadas en su territorio.

2. En estos supuestos de dispositivos móviles, las autorizaciones no se podrán conceder en ningún caso con carácter indefinido o permanente, siendo otorgadas por el plazo adecuado a la naturaleza y las circunstancias derivadas del peligro o evento concreto, por un periodo máximo de un mes prorrogable por otro.

3. En casos de urgencia o necesidad inaplazable será el responsable operativo de las Fuerzas y Cuerpos de Seguridad competentes el que podrá determinar su uso, siendo comunicada tal actuación con la mayor brevedad posible, y siempre en el plazo de 24 horas, al Delegado o Subdelegado del Gobierno o autoridad competente de las comunidades autónomas.

Artículo 18. *Tratamiento y conservación de las imágenes.*

1. Realizada la filmación de acuerdo con los requisitos establecidos en esta Ley Orgánica, si la grabación captara la comisión de hechos que pudieran ser constitutivos de infracciones penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad, a disposición judicial a la mayor brevedad posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

2. Si se captaran hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad pública, se remitirán al órgano competente, de inmediato, para el inicio del oportuno procedimiento sancionador.

3. Las grabaciones serán destruidas en el plazo máximo de tres meses desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, sujetas a una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

Artículo 19. *Régimen disciplinario.*

1. Sin perjuicio de las responsabilidades penales en las que pudieran incurrir, las infracciones a lo dispuesto en esta Ley Orgánica por los miembros de las Fuerzas y Cuerpos de Seguridad, serán sancionadas con arreglo al régimen disciplinario correspondiente a los infractores y, en su defecto, con sujeción al régimen general de sanciones en materia de protección de datos de carácter personal establecido en esta Ley Orgánica.

2. Se considerarán faltas muy graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado, las siguientes infracciones:

a) Alterar o manipular los registros de imágenes y sonidos, siempre que no constituya delito.

b) Permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o utilizar estos para fines distintos de los previstos legalmente.

c) Reproducir las imágenes y sonidos para fines distintos de los previstos en esta Ley Orgánica.

d) Utilizar los medios técnicos regulados en esta Ley Orgánica para fines distintos de los previstos en la misma.

CAPÍTULO III

Derechos de las personas

Sección 1.ª Régimen general

Artículo 20. *Condiciones generales de ejercicio de los derechos de los interesados.*

1. El responsable del tratamiento deberá facilitar al interesado, de forma concisa, inteligible, de fácil acceso y con lenguaje claro y sencillo para todas las personas, incluidas aquellas con discapacidad, toda la información contemplada en el artículo 21, así como la derivada de los artículos 14, 22 a 26 y 39.

Además, el responsable del tratamiento deberá adoptar las medidas necesarias para garantizar al interesado el ejercicio de sus derechos a los que se refieren los artículos 14 y 22 a 26.

2. El interesado, con capacidad de obrar, podrá actuar en su propio nombre y representación o por medio de representantes, de acuerdo con lo previsto en la normativa sobre el procedimiento administrativo común de las Administraciones Públicas.

3. La información será facilitada por cualquier medio adecuado, incluidos los medios electrónicos, procurando utilizar el mismo medio empleado en la solicitud.

4. El responsable del tratamiento informará por escrito al interesado, sin dilación indebida, sobre el curso dado a su solicitud. La solicitud se entenderá desestimada si transcurrido un mes desde su presentación no ha sido resuelta expresamente y notificada al interesado.

5. La información a la que se refiere el apartado 1 se facilitará gratuitamente. Cuando las solicitudes de un interesado sean manifiestamente infundadas o excesivas, en particular debido a su carácter repetitivo, el responsable del tratamiento podrá inadmitirlas a trámite, mediante resolución motivada.

El responsable del tratamiento deberá demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

En todo caso se considerará que la solicitud es repetitiva cuando se realicen tres solicitudes sobre el mismo supuesto durante el plazo de seis meses, salvo que exista causa legítima para ello.

6. Cuando el responsable del tratamiento tenga dudas razonables acerca de la identidad de la persona física que formula la solicitud a la que se refieren los artículos 22 y 23, le requerirá para que facilite la información complementaria que resulte necesaria para confirmar su identidad en el plazo de diez días. Transcurrido dicho plazo sin que se aporte la información, se le tendrá por desistido de su petición mediante resolución motivada. El plazo al que se refiere el apartado 4 comenzará a computarse desde la fecha en la que se facilite dicha información complementaria.

Artículo 21. *Información que debe ponerse a disposición del interesado.*

1. El responsable del tratamiento de los datos pondrá a disposición del interesado, al menos, la siguiente información:

a) La identificación del responsable del tratamiento y sus datos de contacto.

b) Los datos de contacto del delegado de protección de datos, en su caso.

c) Los fines del tratamiento a los que se destinen los datos personales.

d) El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma.

e) El derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, supresión o la limitación de su tratamiento.

2. Además de la información a la que se refiere el apartado 1, atendiendo a las circunstancias del caso concreto, el responsable del tratamiento proporcionará al interesado la siguiente información adicional para permitir el ejercicio de sus derechos:

a) La base jurídica del tratamiento.

b) El plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo.

c) Las categorías de destinatarios de los datos personales, cuando corresponda, en particular, los establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.

d) Cualquier otra información necesaria, en especial, cuando los datos personales se hayan recogido sin conocimiento del interesado.

Artículo 22. *Derecho de acceso del interesado a sus datos personales.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen. En caso de que se confirme el tratamiento, el interesado tendrá derecho a acceder a dichos datos personales, así como a la siguiente información:

a) Los fines y la base jurídica del tratamiento.

b) Las categorías de datos personales de que se trate.

c) Los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales, en particular, los destinatarios establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.

d) El plazo de conservación de los datos personales, cuando sea posible, o, en caso contrario, los criterios utilizados para determinar dicho plazo.

e) La existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de los datos personales relativos al interesado o la limitación de su tratamiento.

f) El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma.

g) La comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen, sin revelar la identidad de ninguna persona física, en especial en el caso de fuentes confidenciales.

2. Cuando el responsable trate una gran cantidad de información relativa al interesado y éste ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá requerir al interesado que concrete la solicitud en el plazo de diez días.

3. Se entenderá concedido el derecho de acceso si el responsable del tratamiento facilita al interesado un sistema remoto, directo y seguro que garantice, de modo permanente, el acceso a la totalidad de sus datos personales. La notificación informando al interesado del procedimiento puesto en marcha a través de este sistema, permitirá denegar su solicitud de acceso efectuada por otras vías.

Si el acceso remoto no facilita la totalidad de la información contenida en el apartado 1, el interesado tendrá derecho a solicitarla.

4. Cuando el interesado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho interesado asumirá el exceso de coste que su elección comporte. En este caso, sólo será exigible al responsable del tratamiento que la satisfacción del derecho de acceso a través del medio propuesto se produzca sin dilaciones indebidas. Si el interesado no asumiera el exceso de coste, se le facilitará el acceso por el medio inicialmente propuesto por el responsable del tratamiento.

Artículo 23. *Derechos de rectificación, supresión de datos personales y limitación de su tratamiento.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento, sin dilación indebida, la rectificación de los datos personales que le conciernen, cuando tales datos resulten inexactos.

Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales cuando estos resulten incompletos.

El interesado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa del carácter incompleto o inexacto de los datos objeto de tratamiento.

2. El responsable del tratamiento, a iniciativa propia o como consecuencia del ejercicio del derecho de supresión del interesado, suprimirá los datos personales sin dilación indebida

y, en todo caso, en el plazo máximo de un mes a contar desde que tenga conocimiento, cuando el tratamiento infrinja los artículos 6, 11 o 13, o cuando los datos personales deban ser suprimidos en virtud de una obligación legal a la que esté sujeto.

3. En lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de los datos personales cuando se dé alguna de las siguientes circunstancias:

a) El interesado ponga en duda la exactitud de los datos personales y no pueda determinarse su exactitud o inexactitud.

b) Los datos personales hayan de conservarse a efectos probatorios.

Cuando el tratamiento esté limitado en virtud de la letra a), el responsable del tratamiento informará al interesado antes de levantar la limitación del tratamiento.

4. En caso de que el responsable del tratamiento rectifique unos datos personales inexactos que provengan de otra autoridad competente, se deberá comunicar a esta la rectificación.

5. Cuando los datos personales hayan sido rectificados o suprimidos o el tratamiento haya sido limitado, el responsable del tratamiento lo notificará a los destinatarios, que deberán rectificar o suprimir los datos personales que estén bajo su responsabilidad o limitar su tratamiento.

Artículo 24. *Restricciones a los derechos de información, acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento.*

1. El responsable del tratamiento podrá aplazar, limitar u omitir la información a la que se refiere el artículo 21.2, así como denegar, total o parcialmente, las solicitudes de ejercicio de los derechos contemplados en los artículos 22 y 23, siempre que, teniendo en cuenta los derechos fundamentales y los intereses legítimos de la persona afectada, resulte necesario y proporcional para la consecución de los siguientes fines:

a) Impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales.

b) Evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.

c) Proteger la seguridad pública.

d) Proteger la Seguridad Nacional.

e) Proteger los derechos y libertades de otras personas.

2. En caso de restricción de los derechos contemplados en los artículos 22 y 23, el responsable del tratamiento informará por escrito al interesado sin dilación indebida, y en todo caso, en el plazo de un mes a contar desde que tenga conocimiento, de dicha restricción, de las razones de la misma, así como de las posibilidades de presentar una reclamación ante la autoridad de protección de datos, sin perjuicio de las restantes acciones judiciales que pueda ejercer en virtud de lo dispuesto en esta Ley Orgánica.

Las razones de la restricción podrán ser omitidas o ser sustituidas por una redacción neutra cuando la revelación de los motivos de la restricción pueda poner en riesgo los fines a los que se refiere el apartado anterior.

3. El responsable del tratamiento documentará los fundamentos de hecho o de derecho en los que se sustente la decisión denegatoria del ejercicio del derecho de acceso. Dicha información estará a disposición de las autoridades de protección de datos.

Artículo 25. *Ejercicio de los derechos del interesado a través de la autoridad de protección de datos.*

1. En los casos en que se produzca un aplazamiento, limitación u omisión de la información a que se refiere el artículo 21 o una restricción del ejercicio de los derechos contemplados en los artículos 22 y 23, en los términos previstos en el artículo 24, el interesado podrá ejercer sus derechos a través de la autoridad de protección de datos competente. El responsable del tratamiento informará al interesado de esta posibilidad.

2. Cuando, en virtud de lo establecido en el apartado anterior, se ejerciten los derechos a través de la autoridad de protección de datos, esta deberá informar al interesado, al menos,

de la realización de todas las comprobaciones necesarias o la revisión correspondiente y de su derecho a interponer recurso contencioso-administrativo.

Sección 2.ª Régimen especial

Artículo 26. *Derechos de los interesados como consecuencia de investigaciones y procesos penales.*

1. El ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento a los que se hace referencia en los artículos anteriores se llevará a cabo de conformidad con las normas procesales penales cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales.

2. Cuando los datos sean objeto de un tratamiento con fines jurisdiccionales del que sea responsable un órgano del orden jurisdiccional penal, o el Ministerio Fiscal, el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento se realizará de conformidad con lo previsto en la Ley Orgánica 6/1985, de 1 de julio, en las normas procesales y en su caso, el Estatuto Orgánico del Ministerio Fiscal.

3. En defecto de regulación del ejercicio de estos derechos en dichas normas, se aplicará lo dispuesto en esta Ley Orgánica.

CAPÍTULO IV

Responsable y encargado de tratamiento

Sección 1.ª Obligaciones generales

Artículo 27. *Obligaciones del responsable del tratamiento.*

1. El responsable del tratamiento, tomando en consideración la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicará las medidas técnicas y organizativas apropiadas para garantizar que el tratamiento se lleve a cabo de acuerdo con esta Ley Orgánica y con lo previsto en la legislación sectorial y en sus normas de desarrollo. Tales medidas se revisarán y actualizarán cuando resulte necesario.

2. Entre las medidas mencionadas en el apartado anterior se incluirá la aplicación de las oportunas políticas de protección de datos, cuando sean proporcionadas en relación con las actividades de tratamiento.

Artículo 28. *Protección de datos desde el diseño y por defecto.*

1. En el momento de determinar los medios para el tratamiento, así como en el momento del tratamiento propiamente dicho, deberán aplicarse las medidas técnicas y organizativas que resulten apropiadas conforme al estado de la técnica y el coste de la aplicación, la naturaleza, el ámbito, el contexto, los fines del tratamiento y los riesgos para los derechos y libertades de las personas físicas. El objetivo será salvaguardar los principios de protección de datos de forma efectiva, al tiempo que integrar las garantías necesarias en el tratamiento. Entre estas medidas técnicas, se podrá adoptar la seudonimización de los datos personales a los efectos de contribuir a la aplicación de los principios establecidos en esta Ley Orgánica, en particular, el de minimización de datos personales.

2. Además, las medidas técnicas y organizativas deberán garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales que resulten necesarios para cada uno de los fines específicos del tratamiento. Dicha obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su período de conservación y a su accesibilidad.

Tales medidas garantizarán que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas sin intervención humana.

Artículo 29. *Supuestos de corresponsabilidad en el tratamiento.*

1. Cuando dos o más responsables del tratamiento determinen conjuntamente los objetivos y los medios de tratamiento serán considerados corresponsables del tratamiento.

2. Salvo que las responsabilidades hayan sido previstas por el Derecho de la Unión Europea o por la legislación española, los corresponsables del tratamiento establecerán, de modo transparente y de mutuo acuerdo, a través del instrumento oportuno, sus respectivas responsabilidades en el cumplimiento de esta Ley Orgánica, en particular, en lo referido al ejercicio de los derechos del interesado y a sus respectivas obligaciones en el suministro de la información contemplada en el artículo 21.

El citado acuerdo designará el punto de contacto para los interesados, a menos que venga ya determinado legalmente.

La concreción de las responsabilidades se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Artículo 30. *Encargado del tratamiento.*

1. Cuando una operación de tratamiento vaya a ser llevada a cabo por cuenta de un responsable del tratamiento, este recurrirá únicamente a encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de esta Ley Orgánica y garantice la protección de los derechos del interesado.

El encargado podrá ser una persona física o jurídica, de naturaleza privada o pública.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito del responsable del tratamiento. El encargado informará siempre al responsable de cualquier cambio previsto referido a la adición o sustitución de otros encargados, pudiendo el responsable oponerse a dichos cambios.

3. El tratamiento por medio de un encargado se regirá por un contrato, convenio u otro instrumento jurídico que corresponda, por escrito, incluyendo la posibilidad del formato electrónico, concluido con arreglo al Derecho de la Unión Europea o a la legislación española. Dicho instrumento jurídico vinculará al encargado con el responsable y fijará el objeto y la duración del tratamiento, su naturaleza y finalidad, el tipo de datos personales y categorías de interesados, así como las obligaciones y derechos del responsable.

El instrumento jurídico estipulará, en particular, que el encargado del tratamiento deberá:

a) Actuar únicamente siguiendo las instrucciones del responsable del tratamiento.

b) Garantizar, a través del instrumento o sistema oportuno, que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación profesional de secreto o confidencialidad.

c) Asistir al responsable del tratamiento por cualquier medio adecuado para garantizar el cumplimiento de las disposiciones sobre los derechos del interesado.

d) Suprimir o devolver, a elección del responsable del tratamiento, todos los datos personales al responsable del tratamiento, una vez finalice la prestación de los servicios de tratamiento, así como suprimir las copias existentes, a menos que el Derecho de la Unión Europea o la legislación española requieran la conservación de los datos personales.

e) Poner a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de estas obligaciones.

f) Respetar las condiciones indicadas en este apartado y en el apartado 2 para contratar a otro encargado del tratamiento.

4. Si un encargado del tratamiento determinase los fines y medios de dicho tratamiento, infringiendo esta Ley Orgánica, será considerado responsable con respecto a ese tratamiento.

5. El encargado del tratamiento se regirá, en lo no previsto por esta Ley Orgánica, por lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 31. *Tratamiento bajo la autoridad del responsable o del encargado del tratamiento.*

El encargado del tratamiento, así como cualquier persona que actúe bajo la autoridad del responsable o del encargado del tratamiento y tenga acceso a datos personales, sólo podrá

someterlos a tratamiento siguiendo instrucciones del responsable del tratamiento, a menos que esté obligado a hacerlo por el Derecho de la Unión Europea o por la legislación española.

Artículo 32. *Registros de las actividades de tratamiento.*

1. Cada responsable debe conservar un registro de todas las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad. Dicho registro deberá contener la información siguiente:

a) La identificación del responsable del tratamiento y sus datos de contacto, así como, en su caso, del corresponsable y del delegado de protección de datos.
b) Los fines del tratamiento.
c) Las categorías de destinatarios a quienes se hayan comunicado o vayan a comunicarse los datos personales, incluidos los destinatarios en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.
d) La descripción de las categorías de interesados y de las categorías de datos personales.
e) El recurso a la elaboración de perfiles, en su caso.
f) Las categorías de transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional, en su caso.
g) La indicación de la base jurídica del tratamiento, así como, en su caso, las transferencias internacionales de las que van a ser objeto los datos personales.
h) Los plazos previstos para la supresión de las diferentes categorías de datos personales, cuando sea posible.
i) La descripción general de las medidas técnicas y organizativas de seguridad a las que se refiere el artículo 37.1, cuando sea posible.

2. Cada encargado del tratamiento llevará un registro de todas las actividades de tratamiento de datos personales efectuadas en nombre de un responsable. Este registro contendrá la información siguiente:

a) El nombre y los datos de contacto del encargado o encargados del tratamiento, de cada responsable del tratamiento en cuyo nombre actúe el encargado y, en su caso, del delegado de protección de datos.
b) Las categorías de tratamientos efectuados en nombre de cada responsable.
c) Las transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional, en su caso, incluida la identificación de dicho Estado o de dicha organización internacional cuando el responsable del tratamiento así lo ordene explícitamente.
d) La descripción general de las medidas técnicas y organizativas de seguridad a las que se refiere el artículo 37.1, cuando sea posible.

3. Los registros referidos en este artículo se establecerán y llevarán por escrito, incluida la posibilidad del formato electrónico.
Estos registros estarán a disposición de la autoridad de protección de datos competente, a solicitud de esta, de conformidad con lo dispuesto legalmente.
4. Los responsables de los tratamientos harán público el registro de sus actividades de tratamiento, accesible por medios electrónicos, en el que constará la información a la que se refiere el apartado 1.

Artículo 33. *Registro de operaciones.*

1. Los responsables y encargados del tratamiento deberán mantener registros de, al menos, las siguientes operaciones de tratamiento en sistemas de tratamiento automatizados: recogida, alteración, consulta, comunicación, incluidas las transferencias, y combinación o supresión. Los registros de consulta y comunicación harán posible determinar la justificación, la fecha y la hora de tales operaciones y, en la medida de lo posible, el nombre de la persona que consultó o comunicó los datos personales, así como la identidad de los destinatarios de dichos datos personales.

2. Estos registros se utilizarán únicamente a efectos de verificar la legalidad del tratamiento, controlar el cumplimiento de las medidas y de las políticas de protección de datos y garantizar la integridad y la seguridad de los datos personales en el ámbito de los procesos penales.

Dichos registros estarán a disposición de la autoridad de protección de datos competente a solicitud de esta, de conformidad con lo dispuesto legalmente.

Artículo 34. *Cooperación con las autoridades de protección de datos.*

El responsable y el encargado del tratamiento cooperarán con la autoridad de protección de datos competente, en el marco de la legislación vigente, cuando esta lo solicite en el desempeño de sus funciones.

Artículo 35. *Evaluación de impacto relativa a la protección de datos.*

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, suponga por su naturaleza, alcance, contexto o fines, un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.

2. La evaluación incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos peligros, así como las medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar su conformidad con esta Ley Orgánica. Esta evaluación tendrá en cuenta los derechos e intereses legítimos de los interesados y de las demás personas afectadas.

3. Las autoridades de protección de datos podrán establecer una lista de tratamientos que estén sujetos a la realización de una evaluación de impacto con arreglo a lo dispuesto en el apartado anterior y, del mismo modo, podrán establecer una lista de tratamientos que no estén sujetos a esta obligación. Ambas listas tendrán un carácter meramente orientativo.

Artículo 36. *Consulta previa a la autoridad de protección de datos.*

1. El responsable o el encargado del tratamiento consultará a la autoridad de protección de datos, antes de proceder al tratamiento de datos personales que vayan a formar parte de un nuevo fichero, en cualquiera de las siguientes circunstancias:

a) Cuando la evaluación del impacto en la protección de los datos indique que el tratamiento entrañaría un alto nivel de riesgo, a falta de medidas adoptadas por el responsable para mitigar el riesgo o los posibles daños.

b) Cuando el tipo de tratamiento pueda generar un alto nivel de riesgo para los derechos y libertades de los interesados, en particular, cuando se usen tecnologías, mecanismos o procedimientos nuevos.

2. La autoridad de protección de datos correspondiente podrá establecer una lista de carácter orientativo, de las operaciones de tratamiento sujetas a consulta previa, con arreglo a lo dispuesto en el apartado anterior.

3. El responsable del tratamiento facilitará a la autoridad de protección de datos competente, la evaluación de impacto contemplada en el artículo 35 y, previa solicitud, cualquier información adicional que permita a dicha autoridad de protección de datos evaluar la conformidad del tratamiento y, más concretamente, el nivel de riesgo para la protección de los datos personales del interesado y las garantías correspondientes.

4. Cuando la autoridad de protección de datos considere que el tratamiento previsto en el apartado 1 pudiera infringir lo dispuesto en esta Ley Orgánica deberá, en un plazo de seis semanas desde la solicitud de la consulta, asesorar por escrito al responsable del tratamiento y, en su caso, al encargado del tratamiento, en especial, cuando el responsable del tratamiento no haya identificado o mitigado suficientemente el peligro o el nivel de riesgo. Asimismo, la autoridad de protección de datos podrá ejercer cualquiera de sus potestades de investigación, corrección o consulta.

Este plazo podrá prorrogarse un mes, en función de la complejidad del tratamiento previsto. La autoridad de protección de datos informará al responsable y, en su caso, al encargado acerca de la prórroga, en el plazo de un mes a partir de la recepción de la solicitud de consulta, junto con los motivos de la dilación.

En caso de no contestar a la consulta en el plazo previsto, no operará la presunción del carácter favorable del mismo.

Sección 2.ª Seguridad de los datos personales

Artículo 37. *Seguridad del tratamiento.*

1. El responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, especialmente en lo relativo al tratamiento de las categorías de datos personales a las que se refiere el artículo 13. En particular, deberán aplicar a los tratamientos de datos personales las medidas incluidas en el Esquema Nacional de Seguridad.

2. Por lo que respecta al tratamiento automatizado, el responsable o encargado del tratamiento, a raíz de una evaluación de los riesgos, pondrá en práctica medidas de control con el siguiente propósito:

a) En el control de acceso a los equipamientos, denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento.

b) En el control de los soportes de datos, impedir que estos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas.

c) En el control del almacenamiento, impedir que se introduzcan sin autorización datos personales, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización.

d) En el control de los usuarios, impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos.

e) En el control del acceso a los datos, garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado, sólo puedan tener acceso a los datos personales para los que han sido autorizados.

f) En el control de la transmisión, garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse, o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos.

g) En el control de la introducción, garantizar que pueda verificarse y constatarse, a posteriori, qué datos personales se han introducido en los sistemas de tratamiento automatizado, en qué momento y quién los ha introducido.

h) En el control del transporte, impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización.

i) En el control de restablecimiento, garantizar que los sistemas instalados puedan restablecerse en caso de interrupción.

j) En el control de fiabilidad e integridad, garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema.

Artículo 38. *Notificación a la autoridad de protección de datos de una violación de la seguridad de los datos personales.*

1. Cualquier violación de la seguridad de los datos personales será notificada por el responsable del tratamiento a la autoridad de protección de datos competente, a menos que sea improbable que la violación de la seguridad de los datos personales constituya un peligro para los derechos y las libertades de las personas físicas.

La notificación deberá realizarse en el plazo de las setenta y dos horas siguientes al momento en que se haya tenido constancia de ella. En caso contrario, deberá ir acompañada de los motivos de la dilación.

2. El encargado del tratamiento notificará, sin dilación indebida, al responsable del tratamiento, las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, al menos:

a) Referir la naturaleza de la violación de la seguridad de los datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de personas afectadas, así como las categorías y el número aproximado de registros de datos personales afectados por la violación de la seguridad.

b) Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Detallar las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar sus posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, se podrá facilitar de forma progresiva, a medida que se disponga de ella.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relativos a dicha violación, sus efectos y las medidas correctivas adoptadas.

Dicha documentación estará a disposición de la autoridad de protección de datos competente al objeto de verificar el cumplimiento de lo dispuesto en este artículo.

6. Cuando la violación de la seguridad de los datos personales afecte a datos que hayan sido transmitidos por el responsable del tratamiento o al responsable del tratamiento de otro Estado miembro de la Unión Europea, la información recogida en el apartado 3 se comunicará al responsable del tratamiento de dicho Estado.

7. Todas las actividades relacionadas en este artículo se realizarán sin dilaciones indebidas.

Artículo 39. *Comunicación de una violación de la seguridad de los datos personales al interesado.*

1. Cuando existan indicios de que una violación de la seguridad de los datos personales supondría un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento comunicará al interesado, sin dilación indebida, la violación de la seguridad de los datos personales.

2. La comunicación al interesado describirá con lenguaje claro, sencillo y accesible conforme a sus circunstancias y capacidades, la naturaleza de la violación de la seguridad de los datos personales y contendrá, al menos, la información y las medidas a las que se refiere el artículo 38.3. b), c) y d).

3. No se efectuará la comunicación al interesado que prevé el apartado 1 cuando se cumpla alguna de las condiciones siguientes:

a) Que el responsable del tratamiento haya adoptado medidas apropiadas de protección técnica y organizativa y dichas medidas se hayan aplicado a los datos personales afectados por la violación de la seguridad antes de la misma, en particular, aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como en el caso del cifrado.

b) Que el responsable del tratamiento haya tomado medidas ulteriores para garantizar que no se materialice el alto nivel de riesgo para los derechos y libertades del interesado a que hace referencia el apartado 1.

c) Que suponga un esfuerzo desproporcionado, en cuyo caso, se optará por su publicación en el boletín oficial correspondiente, en la sede electrónica del responsable del tratamiento o en otro canal oficial que permita una comunicación efectiva con el interesado.

4. En el supuesto de que el responsable del tratamiento no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de protección de datos competente, una vez valorada la existencia de un alto nivel de riesgo, podrá exigirle que proceda a dicha comunicación, o bien que determine la concurrencia de alguna de las condiciones previstas en el apartado 3.

5. La comunicación al interesado referida en el apartado 1 podrá aplazarse, limitarse u omitirse con sujeción a las condiciones y por los motivos previstos en el artículo 24.

Sección 3.ª Delegado de protección de datos

Artículo 40. *Designación del delegado de protección de datos.*

1. Los responsables del tratamiento designarán, en todo caso, un delegado de protección de datos. No estarán obligados a designarlo los órganos jurisdiccionales o el Ministerio Fiscal cuando el tratamiento de datos personales se realice en el ejercicio de sus funciones jurisdiccionales.

2. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales. En concreto, se tendrán en cuenta sus conocimientos especializados en legislación, su experiencia en materia de protección de datos y su capacidad para desempeñar las funciones a las que se refiere el artículo 42. En el caso de haber designado un delegado de protección de datos al amparo del Reglamento General de Protección de Datos, este será el que asumirá las funciones de delegado de protección de datos previstas en esta Ley Orgánica.

3. Podrá designarse a un único delegado de protección de datos para varias autoridades competentes, teniendo en cuenta la estructura organizativa y el tamaño de estas.

4. Los responsables del tratamiento publicarán los datos de contacto del delegado de protección de datos y comunicarán a la autoridad de protección de datos competente su designación y cese, en el plazo de diez días desde que se haya producido.

Artículo 41. *Posición del delegado de protección de datos.*

1. El responsable del tratamiento velará porque el delegado de protección de datos participe adecuada y oportunamente en todas las cuestiones relativas a la protección de datos personales, al tiempo que cuidará de que mantenga sus conocimientos especializados, cuente con los recursos necesarios para el desempeño de sus funciones y acceda a los datos personales y a las operaciones de tratamiento.

2. El delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitar cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento. La existencia de cualquier deber de confidencialidad o secreto no permitirá que el responsable o el encargado del tratamiento se oponga a dicho acceso.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de dirección del responsable o del encargado del tratamiento.

Artículo 42. *Funciones del delegado de protección de datos.*

El responsable del tratamiento encomendará al delegado de protección de datos, al menos, las siguientes funciones:

a) Informar y asesorar al responsable del tratamiento y a los empleados que se ocupen del mismo, acerca de las obligaciones que les incumben en virtud de esta Ley Orgánica y de otras disposiciones de protección de datos aplicables.

b) Supervisar el cumplimiento de lo dispuesto en esta Ley Orgánica y en otras disposiciones de protección de datos aplicables, así como de lo establecido en las políticas del responsable del tratamiento en materia de protección de datos personales, incluidas la

asignación de responsabilidades, la concienciación y formación del personal que participe en las operaciones de tratamiento y las auditorías correspondientes.

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización.

d) Cooperar con la autoridad de protección de datos en los términos de la legislación vigente.

e) Actuar como punto de contacto de la autoridad de protección de datos para las cuestiones relacionadas con el tratamiento, incluida la consulta previa referida en el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

CAPÍTULO V

Transferencias de datos personales a terceros países que no sean miembros de la Unión Europea o a organizaciones internacionales

Artículo 43. *Principios generales de las transferencias de datos personales.*

1. Al objeto de garantizar el nivel de protección de las personas físicas previsto en esta Ley Orgánica, cualquier transferencia de datos personales realizada por las autoridades competentes españolas a un Estado que no sea miembro de la Unión Europea o a una organización internacional, incluidas las transferencias ulteriores a otro Estado que no pertenezca a la Unión Europea o a otra organización internacional, deberá cumplir las siguientes condiciones:

a) Que la transferencia sea necesaria para los fines establecidos en el artículo 1.

b) Que los datos personales sean transferidos a un responsable del tratamiento competente para los fines mencionados en el artículo 1.

c) Que, en caso de que los datos personales hayan sido transferidos a la autoridad competente española procedentes de otro Estado miembro de la Unión Europea, dicho Estado miembro autorice previamente la transferencia ulterior de conformidad con su Derecho nacional.

d) Que la Comisión Europea haya adoptado una decisión de adecuación de acuerdo con el artículo 44 o, a falta de dicha decisión, cuando se hayan aportado o existan garantías apropiadas de conformidad con el artículo 45 o, a falta de ambas, cuando resulten de aplicación las excepciones para situaciones específicas de acuerdo con el artículo 46.

e) Cuando se trate de una transferencia ulterior a un Estado que no sea miembro de la Unión Europea u organización internacional, de datos transferidos inicialmente por una autoridad competente española, esta autorizará la transferencia ulterior, una vez considerados todos los factores pertinentes, entre estos, la gravedad de la infracción penal, la finalidad para la que se transfirieron inicialmente los datos personales y el nivel de protección existente en ese Estado u organización internacional a los que se transfieran ulteriormente los datos personales.

2. Las transferencias de datos personales por las autoridades españolas sin autorización previa de otro Estado miembro, conforme al párrafo 1c), sólo se permitirán si la transferencia de datos personales resulta necesaria para prevenir una amenaza inmediata y grave para la seguridad pública, tanto de un Estado miembro de la Unión Europea como no perteneciente a la misma, o para los intereses fundamentales de un Estado miembro de la Unión Europea, y cuando la autorización previa no pueda conseguirse a su debido tiempo.

Las autoridades españolas informarán sin dilación a la autoridad responsable de conceder la autorización previa, y en todo caso en el plazo máximo de diez días a contar desde que se haya producido la transferencia.

3. Se impulsará el establecimiento de mecanismos de cooperación internacional y de asistencia mutua y se fomentará el intercambio de normativa y de buenas prácticas con los Estados que no sean miembros de la Unión Europea y con las organizaciones internacionales, de manera que se facilite la aplicación efectiva de la legislación sobre la protección de datos personales, inclusive en el ámbito de la resolución de conflictos jurisdiccionales, procurando la participación de todas las partes interesadas.

Artículo 44. *Transferencias basadas en una decisión de adecuación.*

1. Cuando la Comisión Europea, mediante una decisión de adecuación, haya decidido que un Estado que no sea miembro de la Unión Europea, un territorio o uno o varios sectores específicos de dicho Estado, o la organización internacional de que se trate, garantizan un nivel de protección adecuado, podrán realizarse transferencias de datos personales a ese Estado u organización internacional. Dichas transferencias no requerirán ninguna autorización específica.

2. Toda decisión de adecuación de la Comisión Europea que determine que un Estado que no sea miembro de la Unión Europea, un territorio o uno o varios sectores específicos de dicho Estado, o una organización internacional ha dejado de garantizar un nivel de protección adecuado, se entenderá sin perjuicio de las transferencias de datos personales a dicho Estado, territorio o sector del mismo o a la organización internacional de que se trate, en virtud de los artículos 45 y 46.

Artículo 45. *Transferencias mediante garantías apropiadas.*

1. En ausencia de una decisión de adecuación de la Comisión Europea conforme al artículo 44 podrán realizarse transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional cuando concurra alguna de las siguientes circunstancias:

a) Se hayan aportado garantías apropiadas respecto a la protección de datos personales en un instrumento jurídicamente vinculante.

b) Se hayan evaluado, por parte del responsable del tratamiento, todas las circunstancias que concurren en la transferencia de datos personales y se haya concluido que existen garantías apropiadas respecto a la protección de datos personales.

2. El responsable del tratamiento informará a la autoridad de protección de datos competente acerca de las categorías de transferencias a tenor del párrafo 1.b).

3. Cuando las transferencias se basen en lo dispuesto en el párrafo 1.b) deberán documentarse. La documentación se pondrá a disposición de la autoridad de protección de datos competente, previa solicitud, con inclusión de la siguiente información: fecha, hora de la transferencia, información sobre la autoridad competente destinataria, justificación de la transferencia y datos personales transferidos.

Artículo 46. *Excepciones para situaciones específicas.*

1. En ausencia de una decisión de adecuación de la Comisión Europea o de garantías apropiadas de acuerdo con los artículos 44 y 45, podrán realizarse transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional cuando la transferencia sea necesaria por concurrir alguna de las siguientes circunstancias:

a) Para proteger los intereses vitales o los derechos y libertades fundamentales del interesado o de otra persona.

b) Para salvaguardar intereses legítimos del interesado reconocidos por la legislación española.

c) Para prevenir una amenaza grave e inmediata para la seguridad pública de un Estado, tanto miembro de la Unión Europea como no perteneciente a la misma.

d) En casos individuales, a efectos del artículo 1.

e) Para el ejercicio, en un caso individual, de acciones legales o para la defensa frente a ellas en relación con los fines incluidos en el artículo 1.

2. Los datos personales no se transferirán, si la autoridad competente de la transferencia determina que los derechos y libertades fundamentales del interesado prevalecen sobre el interés público en la transferencia, establecido en las letras d) y e) del apartado anterior.

3. Las transferencias basadas en lo dispuesto en este artículo deberán documentarse. Esta documentación quedará a disposición de la autoridad de protección de datos competente, con inclusión de la fecha y la hora de la transferencia, la información sobre la

autoridad competente destinataria, la justificación de la transferencia y los datos personales transferidos.

Artículo 47. *Transferencias directas de datos personales a destinatarios, que no sean autoridades competentes, establecidos en Estados no pertenecientes a la Unión Europea.*

1. Excepcionalmente, en casos particulares y específicos y sin perjuicio de la existencia de un acuerdo internacional entre España y un Estado que no sea miembro de la Unión Europea en el ámbito de la cooperación judicial penal o de la cooperación policial, las autoridades competentes españolas podrán transferir datos personales directamente a destinatarios que no tengan la condición de autoridad competente, establecidos en Estados que no sean miembros de la Unión Europea, siempre que se cumplan las disposiciones de esta Ley Orgánica y se satisfagan todas las condiciones siguientes:

a) Que la transferencia sea estrictamente necesaria para la realización de una función de la autoridad competente que lleva a cabo la transferencia conforme al Derecho de la Unión Europea o a la legislación española, con cualquiera de los fines del artículo 1.

b) Que la autoridad competente que realiza la transferencia determine que ninguno de los derechos y libertades fundamentales del interesado son superiores al interés público que precise de la transferencia de que se trate.

c) Que la autoridad competente que realiza la transferencia considere que la transferencia a una autoridad competente del Estado en el que está establecido el destinatario, con cualquiera de los fines del artículo 1, resultaría ineficaz o inadecuada, en particular porque la transferencia no pueda efectuarse dentro de plazo.

d) Que se informe sin dilación indebida a la autoridad competente para los fines que contempla el artículo 1 de dicho Estado, salvo que esto resulte ineficaz o inadecuado.

e) Que la autoridad competente que realiza la transferencia informe al destinatario de la finalidad o finalidades específicas para las que puede tratar los datos personales, siempre y cuando dicho tratamiento sea necesario.

2. La autoridad competente que realiza la transferencia informará a la autoridad de protección de datos competente acerca de las transferencias efectuadas a tenor de este artículo.

3. Las transferencias basadas en lo dispuesto en este artículo deberán documentarse.

CAPÍTULO VI

Autoridades de Protección de Datos Independientes

Artículo 48. *Autoridades de protección de datos.*

A los efectos de esta Ley Orgánica son autoridades de protección de datos independientes:

a) La Agencia Española de Protección de Datos.

b) Las autoridades autonómicas de protección de datos, exclusivamente en relación a aquellos tratamientos de los que sean responsables en su ámbito de competencia, y conforme a lo dispuesto en el artículo 57.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y en la normativa autonómica aplicable.

Dichas autoridades se regirán por esta Ley Orgánica respecto de los tratamientos sometidos a la misma, de acuerdo con los principios de cooperación institucional, coordinación de criterios e información mutua, y por lo establecido en el Título VII de la Ley Orgánica 3/2018, de 5 de diciembre, y en sus normas de creación, así como por lo que establezcan sus normas de desarrollo.

La Agencia Española de Protección de Datos actuará como representante de las autoridades de protección de datos en el Comité Europeo de Protección de Datos.

Artículo 49. *Funciones.*

1. Las autoridades de protección de datos ejercerán, respecto de los tratamientos sometidos a esta Ley Orgánica, las siguientes funciones:

a) Supervisar y hacer cumplir las disposiciones adoptadas con arreglo a esta Ley Orgánica.

b) Promover la sensibilización y la comprensión de la ciudadanía acerca de los riesgos, normas, garantías y derechos relativos al tratamiento.

c) Asesorar a las Cortes Generales, al Gobierno de la Nación y a los organismos dependientes o vinculados a la Administración General del Estado, así como, de acuerdo con su ámbito competencial, a las Asambleas Legislativas de las comunidades autónomas, los Consejos de Gobierno y los organismos dependientes o vinculados a la Administración de las comunidades autónomas, acerca de las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento.

d) Promover la sensibilización de los responsables y encargados del tratamiento en relación con las obligaciones que les incumben.

e) Facilitar la información solicitada por los interesados sobre el ejercicio de sus derechos en virtud de esta Ley Orgánica y, en su caso, cooperar a tal fin con las autoridades de protección de datos de otros Estados miembros de la Unión Europea.

f) Tramitar y responder las reclamaciones presentadas por un interesado o por una entidad, organización o asociación de conformidad con el artículo 55, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.

g) Controlar, de acuerdo con lo dispuesto en el artículo 25, la licitud del tratamiento e informar al interesado en un plazo razonable sobre el resultado del control o sobre los motivos por los que no se ha llevado a cabo.

h) Cooperar, en particular compartiendo información, con otras autoridades de protección de datos y prestarse asistencia mutua.

i) Llevar a cabo investigaciones sobre la aplicación de esta Ley Orgánica, en particular basándose en la información recibida de otra autoridad de protección de datos u otra autoridad pública.

j) Realizar un seguimiento de acontecimientos que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, de manera concreta sobre el desarrollo de las tecnologías de la información y la comunicación.

k) Prestar asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36.

l) Contribuir a las actividades del Comité Europeo de Protección de Datos.

m) Informar todas las disposiciones legales o reglamentarias que afecten a tratamientos sometidos a esta Ley Orgánica.

2. Las autoridades de protección de datos adoptarán medidas tendentes a facilitar la formulación de las reclamaciones incluidas en el párrafo 1f), tales como proporcionar formularios que puedan cumplimentarse electrónicamente, sin excluir otros medios.

3. El desempeño de las funciones de las autoridades de control no implicará coste alguno para el interesado ni para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de protección de datos podrá negarse a actuar respecto de la solicitud. La carga de la demostración del carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de protección de datos.

Artículo 50. *Potestades.*

Las autoridades de protección de datos tendrán atribuidas, en el ámbito de esta Ley Orgánica, las siguientes potestades:

a) De investigación, incluyendo el acceso a todos los datos que estén siendo tratados por el responsable o el encargado del tratamiento, en los términos previstos por la legislación vigente.

b) De advertencia y control de lo exigido en esta Ley Orgánica, incluida la sanción de las infracciones cometidas, la elaboración de recomendaciones, órdenes de rectificación, supresión o limitación del tratamiento de datos personales o de limitación temporal o definitiva del tratamiento, incluida su prohibición, así como la orden a los responsables del tratamiento de comunicar las vulneraciones de seguridad de los datos a los interesados.

c) De asesoramiento, que comprende la consulta previa prevista en el artículo 36 y la emisión, por propia iniciativa o previa solicitud, de dictámenes destinados a las Cortes Generales o al Gobierno, a otras instituciones u organismos, así como al público en general, acerca de todo asunto relacionado con la protección de datos personales sujeto a esta Ley Orgánica.

Artículo 51. *Asistencia entre autoridades de protección de datos de los Estados miembros de la Unión Europea.*

1. Las autoridades de protección de datos españolas facilitarán la asistencia y cooperación necesaria a las autoridades de protección de datos de otros Estados miembros de la Unión Europea, debiendo responder a las solicitudes de estas sin dilación indebida, y en cualquier caso, en el plazo máximo de un mes desde su recepción. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, así como las solicitudes para llevar a cabo consultas, inspecciones e investigaciones.

2. Las autoridades de protección de datos españolas podrán solicitar, en el ejercicio de sus funciones, la asistencia y cooperación de las autoridades de protección de datos de otros Estados miembros de la Unión Europea.

Las solicitudes deberán contener toda la información necesaria para su contestación, incluidos los motivos y la finalidad de la solicitud. La información intercambiada se utilizará únicamente para el fin para el que haya sido solicitada.

3. Las contestaciones de las autoridades de protección de datos españolas deberán indicar los resultados obtenidos o las medidas adoptadas con base en la solicitud recibida. Estas respuestas serán remitidas en formato electrónico, en la medida de lo posible.

4. La solicitud de asistencia procedente de una autoridad de protección de datos de un Estado miembro de la Unión Europea únicamente podrá negarse a ser atendida, de manera motivada, cuando la autoridad de protección de datos española no sea competente respecto al objeto o a las medidas solicitadas, o bien cuando el hecho de atender la solicitud vulnere la legislación española o el Derecho de la Unión Europea. Se informará, en su caso, de la restricción de los derechos del interesado adoptada en aplicación del artículo 24.

5. Las medidas adoptadas con ocasión de una solicitud de asistencia mutua serán gratuitas, sin perjuicio de que en circunstancias excepcionales puedan pactarse indemnizaciones por gastos específicos derivados de la prestación de la asistencia.

CAPÍTULO VII

Reclamaciones

Artículo 52. *Régimen aplicable a los procedimientos tramitados ante las autoridades de protección de datos.*

1. En el caso de que los interesados aprecien que el tratamiento de los datos personales haya infringido las disposiciones de esta Ley Orgánica o no haya sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 21, 22 y 23 tendrán derecho a presentar una reclamación ante la autoridad de protección de datos.

2. Dichas reclamaciones serán tramitadas por la autoridad de protección de datos competente con sujeción al procedimiento establecido en el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, y, en su caso, a la legislación de las Comunidades Autónomas que resulte de aplicación. Tendrán carácter subsidiario las normas generales sobre los procedimientos administrativos y el régimen jurídico del sector público.

3. En el caso de que la actuación provenga de un órgano judicial o del Ministerio Fiscal cuando se realice el tratamiento con fines jurisdiccionales la responsabilidad se regirá por lo dispuesto en el Título V del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

4. Sin perjuicio de lo dispuesto en el artículo 55, todo interesado tendrá derecho a interponer recurso contencioso-administrativo, de acuerdo con su normativa reguladora, en caso de que la autoridad de protección de datos competente no dicte resolución expresa y se la notifique en el plazo de tres meses.

Artículo 53. *Derecho a indemnización por entes del sector público.*

1. Los interesados tendrán derecho a ser indemnizados por el responsable del tratamiento, o por el encargado del tratamiento cuando formen parte del sector público, en el caso de que sufran daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en esta Ley Orgánica.

2. Cuando quien incumpla lo dispuesto en esta Ley Orgánica tenga la consideración de Administración pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad patrimonial previsto en la normativa sobre el procedimiento administrativo común de las Administraciones públicas y sobre el régimen jurídico del sector público.

3. En el caso de que la actuación provenga de un órgano judicial o del Ministerio Fiscal cuando se realice el tratamiento con fines jurisdiccionales la responsabilidad se regirá por lo dispuesto en el Título V del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Artículo 54. *Derecho a indemnización por encargados del tratamiento del sector privado.*

1. Los interesados que sufran daño o lesión en sus bienes o derechos por parte del encargado del tratamiento que no forme parte del sector público, como consecuencia del incumplimiento de lo dispuesto en esta Ley Orgánica, tendrán derecho a ser indemnizados.

2. El encargado del tratamiento estará obligado a indemnizar todos los daños y perjuicios que cause a los interesados o a terceros como resultado de las operaciones de tratamientos de datos previstas en el contrato u otro instrumento o acto jurídico suscrito con el responsable del tratamiento conforme al artículo 30, de conformidad con el régimen de responsabilidad del contratista por los daños causados a terceros regulado en la normativa sobre contratos del sector público.

3. Cuando tales daños y perjuicios hayan sido ocasionados como consecuencia inmediata y directa de una orden de la autoridad competente responsable del tratamiento, será esta la responsable.

4. Los interesados o los terceros perjudicados podrán requerir al responsable del tratamiento, dentro del año siguiente a la producción del hecho, para que informe, una vez oído el encargado del tratamiento, acerca de a cuál de las partes contratantes o de las que hayan suscrito el acto jurídico conforme al artículo 30, corresponde la responsabilidad de los daños. El ejercicio de esta facultad interrumpe el plazo de prescripción de la acción.

5. Con independencia de lo previsto en los apartados anteriores, el encargado del tratamiento que no forme parte del sector público responderá de los daños y perjuicios que durante las operaciones de tratamiento de datos cause. Deberá hacerlo tanto respecto del responsable del tratamiento, como respecto del interesado o de terceros por incumplimientos de esta Ley Orgánica, de infracciones de preceptos legales o reglamentarios, o por el incumplimiento de las previsiones contenidas en el contrato o en otro acto jurídico suscrito. El encargado del tratamiento que no forme parte del sector público deberá haber incurrido en actuaciones que le sean imputables, sin perjuicio de la aplicación del régimen sancionador, en su caso.

Artículo 55. *Tutela judicial efectiva.*

1. Sin perjuicio de cualquier otro recurso administrativo o reclamación, toda persona física o jurídica tendrá derecho a recurrir ante la jurisdicción contencioso-administrativa, de acuerdo con su legislación reguladora, contra los actos y resoluciones dictadas por la autoridad de protección de datos competente.

2. El interesado podrá conferir su representación a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los

derechos y libertades de los interesados en materia de protección de sus datos personales, para que ejerza los derechos contemplados en el apartado anterior.

CAPÍTULO VIII

Régimen sancionador

Artículo 56. *Sujetos responsables.*

1. La responsabilidad por las infracciones cometidas recaerá directamente en los sujetos obligados que, por acción u omisión, realizaran la conducta en que consista la infracción.
2. Están sujetos al régimen sancionador:

a) Los responsables de los tratamientos.
b) Los encargados de los tratamientos.
c) Los representantes de los encargados no establecidos en el territorio de la Unión Europea.
d) El resto de las personas físicas o jurídicas obligadas por el contenido del deber de colaboración establecido en el artículo 7.

3. No será de aplicación el régimen sancionador establecido en este capítulo al delegado de protección de datos.

Artículo 57. *Concurso de normas.*

1. Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de esta u otra Ley, siempre que no constituyan infracciones al Reglamento General de Protección de Datos, ni a la Ley Orgánica 3/2018, de 5 de diciembre, se sancionarán observando las siguientes reglas:

a) El precepto especial se aplicará con preferencia al general.
b) El precepto más amplio o complejo absorberá el que sancione las infracciones subsumidas en aquel.
c) En defecto de los criterios anteriores, se aplicará el precepto que sancione los hechos con la sanción mayor.

2. En el caso de que un solo hecho constituya dos o más infracciones, o cuando una de ellas sea medio necesario para cometer la otra, la conducta será sancionada por aquella infracción que conlleve una mayor sanción.

Artículo 58. *Infracciones muy graves.*

Son infracciones muy graves:

a) El tratamiento de datos personales que vulnere los principios y garantías establecidos en el artículo 6 o sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 11, siempre que se causen perjuicios de carácter muy grave a los interesados.
b) El acceso, cesión, alteración y divulgación de los datos al margen de los supuestos autorizados por el responsable o encargado de los datos, siempre que no constituya ilícito penal.
c) La transferencia temporal o definitiva de datos de carácter personal con destino a Estados que no sean miembros de la Unión Europea o a destinatarios que no sean autoridades competentes, establecidos en dichos Estados incumpliendo las condiciones previstas en los artículos 43 y 47.
d) La utilización de los datos para una finalidad que no sea compatible con el objetivo para el que fueron recogidos o cuando no se cumplan las condiciones establecidas en el artículo 6, siempre que no se cuente con una base legal para ello.
e) El tratamiento de datos personales de las categorías especiales sin que concurra alguna de las circunstancias previstas en el artículo 13 o sin garantizar las medidas de seguridad adecuadas, que cause perjuicios graves a los interesados.

f) La omisión del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal conforme a lo dispuesto en esta Ley Orgánica.

g) La vulneración del deber de confidencialidad del encargado del tratamiento, establecido en el artículo 30.

h) La adopción de decisiones individuales automatizadas sin las garantías señaladas en el artículo 14, siempre que se causen perjuicios de carácter muy grave para los interesados.

i) El impedimento, la obstaculización o la falta de atención reiterada del ejercicio de los derechos del interesado de acceso, rectificación, supresión de sus datos o limitación del tratamiento, siempre que se causen perjuicios de carácter muy grave para los interesados.

j) La negativa a proporcionar a las autoridades competentes la información necesaria para la prevención, detección, investigación y enjuiciamiento de infracciones penales, para la ejecución de sanciones penales o para la protección y prevención frente a las amenazas contra la seguridad pública de acuerdo con lo previsto en el artículo 7, así como a informar al interesado cuando se comuniquen sus datos en virtud del deber de colaboración establecido en dicho artículo.

k) La resistencia u obstrucción del ejercicio de la función inspectora de las autoridades de protección de datos competentes.

l) La falta de notificación a las autoridades de protección de datos competentes acerca de una violación de la seguridad de los datos personales, cuando sea exigible, así como la ausencia de comunicación al interesado de una violación de la seguridad cuando sea procedente de acuerdo con el artículo 39, siempre que se deriven perjuicios de carácter muy grave para el interesado.

m) El incumplimiento de las resoluciones dictadas por las autoridades de protección de datos competentes, en el ejercicio de las potestades que le confiere el artículo 50.

n) No facilitar el acceso del personal de las autoridades de protección de datos competentes a los datos personales, información, locales, equipos y medios de tratamiento, cuando sean requeridos por las mismas, en el ejercicio de sus poderes de investigación.

ñ) El incumplimiento de los plazos de conservación y revisión establecidos en virtud del artículo 8.

Artículo 59. *Infracciones graves.*

Son infracciones graves:

a) El tratamiento de los datos de carácter personal cuando se incumplan los principios del artículo 6 o las condiciones de licitud del tratamiento del artículo 11, siempre que no constituya una infracción muy grave.

b) El tratamiento de datos personales de las categorías especiales sin que concurra alguna de las circunstancias previstas en el artículo 13 o sin garantizar las medidas de seguridad adecuadas, siempre que no constituya una infracción muy grave.

c) La adopción de decisiones individuales automatizadas sin las garantías señaladas en el artículo 14, siempre que no constituya una infracción muy grave.

d) La falta de designación de un delegado de protección de datos en los términos previstos en el artículo 40 o no posibilitar la efectiva participación del mismo en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

e) El incumplimiento de la puesta a disposición al interesado de la información prevista en el artículo 21 o del deber de comunicación al mismo, o a la autoridad de protección de datos competente, de una violación de la seguridad de los datos, que entrañe un grave perjuicio para los derechos y libertades del interesado.

f) La ausencia de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos, incluidas las medidas oportunas desde el diseño y por defecto, así como para integrar las garantías necesarias en el tratamiento.

g) El impedimento, la falta de atención o la obstaculización de los derechos del interesado de acceso, rectificación, supresión de sus datos o limitación del tratamiento, siempre que no constituya infracción muy grave.

h) El incumplimiento de la obligación de llevanza de los registros de actividades de tratamiento o del registro de operaciones de tratamiento, si se causan perjuicios de carácter grave a los interesados.

i) El incumplimiento de las estipulaciones recogidas en el contrato u acto jurídico que vincula al responsable y al encargado del tratamiento, salvo en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento, así como el incumplimiento de las obligaciones impuestas en el artículo 30.

j) La falta de colaboración diligente con las autoridades competentes en el cumplimiento de las obligaciones establecidas en el artículo 7, cuando no constituya una infracción muy grave.

k) La falta de cooperación, la actuación negligente o el impedimento de la función inspectora de las autoridades de protección de datos competentes, cuando no constituya infracción muy grave.

l) El incumplimiento de la evaluación de impacto en la protección de los datos de carácter personal, si se derivan perjuicios o riesgos de carácter grave para los interesados.

m) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos competente, en los casos en que dicha consulta resulte preceptiva conforme al artículo 36.

Artículo 60. *Infracciones leves.*

Son infracciones leves:

a) La afectación leve de los derechos de los interesados como consecuencia de la ausencia de la debida diligencia o del carácter inadecuado o insuficiente de las medidas técnicas y organizativas que se hubiesen implantado.

b) El incumplimiento del principio de transparencia de la información o del derecho de información del interesado establecido en el artículo 21 cuando no se facilite toda la información exigida en esta Ley Orgánica.

c) La inobservancia de la obligación de informar al interesado y a los destinatarios a los que se hayan comunicado o de los que procedan los datos personales rectificados, suprimidos o respecto de los que se haya limitado el tratamiento, conforme a lo establecido en el artículo 23.

d) El incumplimiento de la llevanza de registros de actividades de tratamiento o del registro de operaciones o que los mismos no incorporen toda la información exigida legalmente, siempre que no constituya infracción grave.

e) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando fuera exigible legalmente.

f) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas, a propósito del tratamiento de datos personales y de sus relaciones con los interesados, así como la inexactitud o la falta de concreción en la determinación de las mismas.

g) El incumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de una posible infracción de las disposiciones de esta Ley Orgánica, como consecuencia de una instrucción recibida de este.

h) La notificación incompleta o defectuosa a la autoridad de protección de datos competente de la información relacionada con una violación de seguridad de los datos personales, el incumplimiento de la obligación de documentarla o del deber de comunicar al interesado su existencia, cuando no constituya una infracción grave.

i) La aportación de información inexacta o incompleta a la autoridad de protección de datos competente, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa.

j) La falta de publicación de los datos de contacto del delegado de protección de datos, o la ausencia de comunicación de su designación y cese a la autoridad de protección de datos competente, de conformidad con el artículo 40, cuando su nombramiento sea exigible de acuerdo con esta Ley Orgánica.

Artículo 61. *Régimen jurídico.*

1. El ejercicio de la potestad sancionadora que corresponde a las autoridades de protección de datos competentes, se regirá por lo dispuesto en el presente capítulo, por los títulos VII y IX de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, en cuanto no la contradiga, con carácter supletorio, por la normativa sobre el procedimiento administrativo común de las Administraciones Públicas y el régimen jurídico del sector público.

2. En el supuesto de las infracciones recogidas en los artículos 58. j) y 59. j), el ejercicio de la potestad sancionadora corresponderá respectivamente, a las personas titulares de la Secretaría de Estado de Seguridad y de las Delegaciones del Gobierno. Estos procedimientos se regirán por la normativa sobre procedimiento administrativo común de las Administraciones Públicas y el régimen jurídico del sector público, sin perjuicio de las especialidades que se recogen en este capítulo.

Artículo 62. *Sanciones.*

Por la comisión de las infracciones tipificadas en esta Ley Orgánica se impondrán las siguientes sanciones:

1. En caso de que el sujeto responsable sea algunos de los enumerados en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, se impondrán las sanciones y se adoptarán las medidas establecidas en dicho artículo.

2. En caso de que el sujeto infractor sea distinto de los señalados en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, podrá ser sancionado, con multa de la siguiente cuantía:

a) Las infracciones muy graves, con multa de 360.001 a 1.000.000 euros.
b) Las infracciones graves, con multa de 60.001 a 360.000 euros.
c) Las leves, con multa de 6.000 a 60.000 euros.

A efectos de la determinación de la cuantía de la sanción, se tendrán en cuenta los criterios establecidos en el artículo 83.2 del Reglamento General de Protección de Datos y en el artículo 76.2 de la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 63. *Prescripción de las infracciones y sanciones.*

1. Las infracciones administrativas tipificadas en esta Ley Orgánica prescribirán a los seis meses, a los dos o a los tres años de haberse cometido, según sean leves, graves o muy graves, respectivamente.

Los plazos señalados en esta Ley Orgánica se computarán desde el día en que se haya cometido la infracción. No obstante, en los casos de infracciones continuadas o permanentes, los plazos se computarán desde que finalizó la conducta infractora.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Se interrumpirá igualmente la prescripción como consecuencia de la apertura de un procedimiento judicial penal, hasta que la autoridad judicial comunique al órgano administrativo su finalización.

2. Las sanciones impuestas por infracciones muy graves prescribirán a los tres años, las impuestas por infracciones graves, a los dos años, y las impuestas por infracciones leves al año, computados desde el día siguiente a aquel en que adquiera firmeza en vía administrativa la resolución por la que se impone la sanción.

La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 64. *Caducidad del procedimiento.*

1. El procedimiento caducará transcurridos seis meses desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concurra identidad de sujeto, hecho y fundamento, hasta la finalización de este.

2. La resolución que declare la caducidad se notificará al interesado y pondrá fin al procedimiento, sin perjuicio de que la administración pueda acordar la incoación de un nuevo procedimiento en tanto no haya prescrito la infracción. Los procedimientos caducados no interrumpirán el plazo de prescripción.

Artículo 65. *Carácter subsidiario del procedimiento administrativo sancionador respecto del penal.*

1. No podrán sancionarse los hechos que hayan sido sancionados penal o administrativamente cuando se aprecie identidad de sujeto, de hecho y de fundamento.

2. En los supuestos en que las conductas pudieran ser constitutivas de delito, el órgano administrativo pasará el tanto de culpa a la autoridad judicial o al Ministerio Fiscal y se abstendrá de seguir el procedimiento sancionador mientras la autoridad judicial no dicte sentencia firme o resolución que de otro modo ponga fin al procedimiento penal, o el Ministerio Fiscal no acuerde la improcedencia de iniciar o proseguir las actuaciones en vía penal, quedando hasta entonces interrumpido el plazo de prescripción.

La autoridad judicial y el Ministerio Fiscal comunicarán al órgano administrativo la resolución o acuerdo que hubieran adoptado.

3. De no haberse estimado la existencia de ilícito penal, o en el caso de haberse dictado resolución de otro tipo que ponga fin al procedimiento penal, podrá iniciarse o proseguir el procedimiento sancionador. En todo caso, el órgano administrativo quedará vinculado por los hechos declarados probados en vía judicial.

4. Las medidas cautelares adoptadas antes de la intervención judicial podrán mantenerse mientras la autoridad judicial no resuelva otra cosa.

Disposición adicional primera. *Regímenes específicos.*

1. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad, por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, para los fines previstos en al artículo 1, se regirá por esta Ley Orgánica, sin perjuicio de los requisitos establecidos en regímenes legales especiales que regulan otros ámbitos concretos como el procesal penal, la regulación del tráfico o la protección de instalaciones propias.

2. Fuera de estos supuestos, dichos tratamientos se regirán por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y por la Ley Orgánica 3/2018, de 5 de diciembre.

Disposición adicional segunda. *Intercambio de datos dentro de la Unión Europea.*

El intercambio de datos personales por parte de las autoridades competentes españolas en el interior de la Unión Europea, cuando el Derecho de la Unión Europea o la legislación española exijan dicho intercambio, no estará limitado ni prohibido por motivos relacionados con la protección de las personas físicas respecto al tratamiento de sus datos personales.

Disposición adicional tercera. *Acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial.*

Los acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial que impliquen la transferencia de datos personales a Estados que no sean miembros de la Unión Europea u organizaciones internacionales y que hubieran sido celebrados por España antes del 6 de mayo de 2016, cumpliendo lo dispuesto en el

Derecho de la Unión Europea aplicable antes de dicha fecha, seguirán en vigor hasta que sean objeto de modificación, enmienda o terminación.

Disposición adicional cuarta. *Ficheros y Registro de Población de las Administraciones Públicas.*

1. Las autoridades competentes podrán solicitar al Instituto Nacional de Estadística y a los órganos estadísticos de ámbito autonómico, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del documento de identidad, nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en el padrón municipal de habitantes y en el censo electoral correspondiente a los territorios donde ejerzan sus competencias. Esta solicitud deberá estar motivada en base a cualquiera de los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

2. Los datos obtenidos tendrán como único propósito el cumplimiento de los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, así como de protección y de prevención frente a las amenazas contra la seguridad pública y la comunicación de estas autoridades con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas.

Disposición adicional quinta. *Referencias normativas.*

Las referencias contenidas en normas vigentes en relación a las disposiciones que se derogan expresamente, deberán entenderse efectuadas a los artículos de esta Ley Orgánica que regulan la misma materia que aquellas.

Disposición transitoria única. *Duración del mandato inicial de la persona titular de la Dirección de Supervisión y Control de Protección de datos del Consejo General del Poder Judicial.*

La duración del mandato del primer nombramiento de la persona titular de la Dirección de Supervisión y Control de Protección de datos del Consejo General del Poder Judicial será de tres años no renovable.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas todas las normas de igual o inferior rango en lo que contradigan o se opongan a lo dispuesto en esta Ley Orgánica.

Disposición final primera. *Modificación de la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria.*

Se introduce un nuevo artículo 15 bis en la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria, que queda redactado como sigue:

> **«Artículo 15 bis.** *Tratamientos de datos de carácter personal.*
>
> 1. Admitido en el establecimiento un interno, se procederá a verificar su identidad personal, efectuando la reseña alfabética, dactilar y fotográfica, así como a la inscripción en el libro de ingresos y a la apertura de un expediente personal relativo a su situación procesal y penitenciaria, respecto del que se reconoce el derecho de acceso. Este derecho sólo se verá limitado de forma individualizada y fundamentada en concretas razones de seguridad o tratamiento.
>
> 2. El tratamiento de los datos personales de los internos se regirá por lo previsto en la Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Los datos personales de categorías especiales que no figuren en el apartado anterior se podrán tratar con el consentimiento del interesado. Sólo se prescindirá de dicho consentimiento cuando sea estrictamente necesario y se efectúe con las garantías adecuadas para proteger el derecho a la

protección de datos de los interesados, atendiendo al tipo de datos que se traten y a las finalidades de los distintos tratamientos dirigidos a la ejecución de la pena.

3. Igualmente se procederá al cacheo de su persona y al registro de sus efectos, retirándose los enseres y objetos no autorizados.

4. En el momento del ingreso se adoptarán las medidas de higiene personal necesarias, entregándose al interno las prendas de vestir adecuadas que precise, firmando el mismo su recepción.»

Disposición final segunda. *Modificación de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal.*

Uno. Se modifica el artículo 12 para incluir en nuevo apartado n) con la siguiente redacción:

«n) La Unidad de Supervisión y Control de Protección de Datos.»

Dos. Se modifica el artículo 20 incluyendo un nuevo apartado Cuatro con la siguiente redacción:

«Cuatro. En la Fiscalía General del Estado, de igual modo, existirá la Unidad de Supervisión y Control de Protección de Datos que ejercerá las competencias que corresponden a la autoridad de protección de datos con fines jurisdiccionales sobre el tratamiento de los mismos realizado por el Ministerio Fiscal, de acuerdo con lo establecido en el artículo 236 octies de la Ley Orgánica del Poder Judicial en el ámbito de sus competencias y facultades. Su regulación se remitirá a los términos previstos en la Ley Orgánica del Poder Judicial en cuanto le sea de aplicación.

Al frente de la Unidad de Supervisión y Control de Protección de Datos se nombrará por mayoría absoluta del Pleno del Consejo Fiscal una persona titular de la Unidad, de entre juristas de reconocida competencia con al menos quince años de ejercicio profesional y con conocimientos y experiencia acreditados en materia de protección de datos.

La duración del mandato de la persona titular de la Unidad de Supervisión y Control de Protección de Datos será de cinco años, no renovable. Durante su mandato permanecerá, en su caso, en situación de servicios especiales y ejercerá exclusivamente las funciones inherentes a su cargo. Sólo podrá ser cesada por incapacidad o incumplimiento grave de sus deberes, apreciados por el Pleno mediante mayoría absoluta.

El régimen de incompatibilidades de la persona titular de la Unidad de Supervisión y Control de Protección de Datos será el mismo que el establecido para los Fiscales al servicio de los órganos técnicos de la Fiscalía General del Estado. La persona titular de la Unidad de Supervisión y Control de Protección de Datos deberá ejercer sus funciones con absoluta independencia y neutralidad.

La persona titular y el resto de personal adscrito a la Unidad de Supervisión y Control de Protección de Datos estarán sujetos al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus atribuciones. Este deber de secreto profesional se aplicará en particular a la información que faciliten las personas físicas a la Unidad de Supervisión y Control de Protección de Datos en materia de infracciones de la presente normativa.

La composición, organización y funcionamiento de la Unidad de Supervisión y Control de Protección de Datos será regulada reglamentariamente. Se deberá velar porque la Unidad cuente, en todo caso, con todos los medios personales y materiales necesarios para el adecuado ejercicio de sus funciones.»

Tres. Se modifica el artículo 14 para incluir en el apartado 4 una nueva letra l) con el contenido siguiente:

«l) Nombrar por mayoría absoluta a la persona titular de la Unidad de Supervisión y Control de Protección de Datos.»

Disposición final tercera. *Modificación de la Ley Orgánica 6/1985 de 1 de julio, del Poder Judicial.*

Los artículos que se relacionan quedarán modificados en los términos siguientes:

Uno. El artículo 234 queda redactado como sigue:

«Artículo 234.

1. Los Letrados de la Administración de Justicia y funcionarios competentes de la oficina judicial y de la oficina fiscal facilitarán a los interesados cuanta información soliciten sobre el estado de las actuaciones procesales, que podrán examinar y conocer, salvo que sean o hubieren sido declaradas secretas o reservadas conforme a la ley.

2. Las partes y cualquier persona que acredite un interés legítimo y directo tendrán derecho a obtener, en la forma dispuesta en las leyes procesales y, en su caso, en la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, copias simples de los escritos y documentos que consten en los autos, no declarados secretos ni reservados. También tendrán derecho a que se les expidan los testimonios y certificados en los casos y a través del cauce establecido en las leyes procesales.»

Dos. El artículo 235 queda redactado como sigue:

«Artículo 235.

El acceso a las resoluciones judiciales, o a determinados extremos de las mismas, o a otras actuaciones procesales, por quienes no son parte en el procedimiento y acrediten un interés legítimo y directo, podrá llevarse a cabo previa disociación, anonimización u otra medida de protección de los datos de carácter personal que las mismos contuvieren y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda.»

Tres. El artículo 235 bis queda redactado como sigue:

«Artículo 235 bis.

1. Es público el acceso a los datos personales contenidos en los fallos de las sentencias firmes condenatorias, cuando se hubieren dictado en virtud de los delitos previstos en los siguientes artículos:

a) Los artículos 305, 305 bis y 306 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

b) Los artículos 257 y 258 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, cuando el acreedor defraudado hubiese sido la Hacienda Pública.

c) El artículo 2 de la Ley Orgánica 12/1995, de 12 de diciembre, de Represión del Contrabando, siempre que exista un perjuicio para la Hacienda Pública estatal o de la Unión Europea.

2. En los casos previstos en el apartado anterior, el Letrado de la Administración de Justicia emitirá certificado en el que se harán constar los siguientes datos:

a) Los que permitan la identificación del proceso judicial.

b) Nombre y apellidos o denominación social del condenado y, en su caso, del responsable civil.

c) Delito por el que se le hubiera condenado.

d) Las penas impuestas.

e) La cuantía correspondiente al perjuicio causado a la Hacienda Pública por todos los conceptos, según lo establecido en la sentencia.

Mediante diligencia de ordenación el Letrado de la Administración de Justicia ordenará su publicación en el «Boletín Oficial del Estado».

3. Lo dispuesto en este artículo no será de aplicación en el caso de que el condenado o, en su caso, el responsable civil, hubiera satisfecho o consignado en la cuenta de depósitos y consignaciones del órgano judicial competente la totalidad de la cuantía correspondiente al perjuicio causado a la Hacienda Pública por todos los conceptos, con anterioridad a la firmeza de la sentencia.»

Cuatro. El artículo 236 queda redactado como sigue:

«Artículo 236.

La publicidad de los edictos se realizará a través del Tablón Edictal Judicial Único, en la forma en que se disponga reglamentariamente, incluyendo los datos estrictamente necesarios para cumplir con su finalidad.»

Cinco. El artículo 236 bis queda redactado como sigue:

«Artículo 236 bis.

1. El tratamiento de los datos personales podrá realizarse con fines jurisdiccionales o no jurisdiccionales. Tendrá fines jurisdiccionales el tratamiento de los datos que se encuentren incorporados a los procesos que tengan por finalidad el ejercicio de la actividad jurisdiccional.

2. El tratamiento de los datos personales en la Administración de Justicia se llevará cabo por el órgano competente y, dentro de él, por quien tenga la competencia atribuida por la normativa vigente.»

Seis. El artículo 236 ter queda redactado como sigue:

«Artículo 236 ter.

1. El tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo, sin perjuicio de las especialidades establecidas en el presente Capítulo y en las leyes procesales.

2. En el ámbito de la jurisdicción penal, el tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos, diligencias o expedientes de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en la Ley Orgánica de protección de datos personales tratados con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, sin perjuicio de las especialidades establecidas en el presente Capítulo y en las leyes procesales y, en su caso, en la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

3. No será necesario el consentimiento del interesado para que se proceda al tratamiento de los datos personales en el ejercicio de la actividad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba.»

Siete. El artículo 236 quáter queda redactado como sigue:

«Artículo 236 quáter.

Cuando se proceda al tratamiento con fines no jurisdiccionales se estará a lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo.»

Ocho. El artículo 236 quinquies queda redactado como sigue:

«Artículo 236 quinquies.

1. Las resoluciones y actuaciones procesales deberán contener los datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, en especial para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión.

2. Los Jueces y Magistrados, los Fiscales y los Letrados de la Administración de Justicia, conforme a sus competencias, podrán adoptar las medidas que sean necesarias para la supresión de los datos personales de las resoluciones y de los documentos a los que puedan acceder las partes durante la tramitación del proceso siempre que no sean necesarios para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión.

3. Los datos personales que las partes conocen a través del proceso deberán ser tratados por éstas de conformidad con la normativa general de protección de datos. Esta obligación también incumbe a los profesionales que representan y asisten a las partes, así como a cualquier otro que intervenga en el procedimiento.

4. Se deberán comunicar a los órganos competentes dependientes del Consejo General del Poder Judicial, de la Fiscalía General del Estado y del Ministerio de Justicia, en lo que proceda, los datos tratados con fines jurisdiccionales que sean estrictamente necesarios para el ejercicio de las funciones de inspección y control establecidas en esta Ley, y su normativa de desarrollo. También se deberán facilitar los datos tratados con fines no jurisdiccionales cuando ello esté justificado por la interposición de un recurso o sea necesario para el ejercicio de las competencias que tengan legalmente atribuidas.

5. Las Oficinas de Comunicación establecidas en esta Ley, en el ejercicio de sus funciones de comunicación institucional, deberán velar por el respeto del derecho fundamental a la protección de datos personales de aquellos que hubieran intervenido en el procedimiento de que se trate. Para cumplir con su finalidad, podrán recabar los datos necesarios de las autoridades competentes.

6. Los Letrados de la Administración de Justicia deberán facilitar a la Abogacía del Estado los datos personales, la información y los documentos que sean requeridos para el desempeño de la representación y defensa del Reino de España ante el Tribunal Europeo de Derechos Humanos y otros órganos internacionales en materia de protección de derechos Humanos, en particular ante el Comité de Naciones Unidas. A tales efectos, se establecerán igualmente los mecanismos de comunicación con la Fiscalía General del Estado, a través de sus unidades competentes.»

Nueve. El artículo 236 sexies queda redactado como sigue:

«Artículo 236 sexies.

1. La Administración competente deberá suministrar los medios tecnológicos adecuados para que se proceda al tratamiento de los datos personales conforme a las disposiciones legales y reglamentarias.

2. La Administración competente deberá cumplir con las responsabilidades que en materia de tratamiento y protección de datos personales se le atribuya como administración prestacional.

3. Se deberán adoptar las medidas organizativas adecuadas para que la Oficina judicial y fiscal realice un adecuado tratamiento de los datos personales. Previo informe del Consejo General del Poder judicial, y, en su caso, de la Fiscalía General del Estado, el Ministerio de Justicia deberá elaborar y actualizar los códigos de conducta destinados a contribuir a la correcta aplicación de la normativa de protección de datos personales en la Oficina judicial y fiscal, adecuando los principios de la normativa general a los propios de la regulación procesal y organización de la Oficina judicial y fiscal.

4. El Ministerio de Justicia y las Comunidades Autónomas con competencias en la materia, dentro de las políticas de apoyo a la Administración de Justicia y desarrollo de la gestión electrónica de los procedimientos, podrán realizar el

tratamiento de datos no personales para el ejercicio de sus competencias de gestión pública, incluyendo el desarrollo e implementación de sistemas automáticos de clasificación documental orientados a la tramitación procesal, con cumplimiento de la normativa de interoperabilidad, seguridad y protección de datos que resulte aplicable.»

Diez. El artículo 236 septies queda redactado como sigue:

«Artículo 236 septies.

1. En relación con el tratamiento de los datos personales con fines jurisdiccionales, los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación al proceso en que los datos fueron recabados. Estos derechos deberán ejercitarse ante los órganos judiciales, fiscalías u Oficina judicial en los que se tramita el procedimiento, y las peticiones deberán resolverse por quien tenga la competencia atribuida en la normativa orgánica y procesal.

2. En todo caso se denegará el acceso a los datos objeto de tratamiento con fines jurisdiccionales cuando las diligencias procesales en que se haya recabado la información sean o hayan sido declaradas secretas o reservadas.

3. En relación con el tratamiento de los datos personales con fines no jurisdiccionales, los interesados podrán ejercitar los derechos de información, acceso, rectificación, supresión, oposición y limitación en los términos establecidos en la normativa general de protección de datos.»

Once. El artículo 236 octies queda redactado como sigue:

«Artículo 236 octies.

1. Respecto a las operaciones de tratamiento efectuadas con fines jurisdiccionales por los Juzgados, Tribunales, Fiscalías, y las Oficinas judicial y fiscal, corresponderán al Consejo General del Poder Judicial y a la Fiscalía General del Estado, en el ámbito de sus respectivas competencias, las siguientes funciones:

a) Supervisar el cumplimiento de la normativa de protección de datos personales mediante el ejercicio de la labor inspectora otorgada en la presente Ley y el Estatuto Orgánico del Ministerio Fiscal.

b) Promover la sensibilización de los profesionales de la Administración de Justicia y su comprensión de los riesgos, normas, garantías, derechos y obligaciones en relación con el tratamiento.

c) Emitir informe sobre los códigos de conducta destinados a contribuir a la correcta aplicación de la normativa de protección de datos personales en la Oficina judicial y fiscal.

d) Previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en materia de protección de datos.

e) Tramitar y responder las reclamaciones presentadas por un interesado o por asociaciones, organizaciones y entidades que tengan capacidad procesal o legitimación para defender intereses colectivos, en los términos que determinen las leyes de aplicación al proceso en que los datos fueron recabados. Se informará al reclamante sobre el curso y resultado de la reclamación en un plazo razonable, previa realización de la investigación oportuna si se considera necesario.

2. Los tratamientos de datos con fines no jurisdiccionales estarán sometidos a la competencia de la Agencia Española de Protección de Datos, que también supervisará el cumplimiento de aquellos tratamientos que no sean competencia de las autoridades indicadas en el apartado anterior.

3. El Consejo General del Poder Judicial, la Fiscalía General del Estado y la Agencia Española de Protección de Datos colaborarán en aras del adecuado ejercicio de las respectivas competencias que la presente Ley Orgánica les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

4. Cuando con ocasión de la realización de actuaciones de investigación relacionadas con la posible comisión de una infracción de la normativa de protección de datos, las autoridades competentes a las que se refieran los apartados anteriores apreciasen la existencia de indicios que supongan la competencia de otra autoridad, darán inmediatamente traslado a esta última a fin de que prosiga con la tramitación del procedimiento.»

Doce. El artículo 236 nonies, queda redactado como sigue:

«Artículo 236 nonies.

1. Las competencias que corresponden a la autoridad de protección de datos personales con fines jurisdiccionales serán ejercidas respecto del tratamiento de los mismos realizado por Juzgados y Tribunales de acuerdo con lo establecido en el artículo 236 octies, por la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial.

2. Al frente de la Dirección de Supervisión y Control de Protección de Datos se nombrará por mayoría absoluta del Pleno del Consejo General del Poder Judicial una persona titular de la Dirección, de entre juristas de reconocida competencia con al menos quince años de ejercicio profesional y con conocimientos y experiencia acreditados en materia de protección de datos.

3. La duración del mandato de la persona titular de la Dirección de Supervisión y Control de Protección de Datos será de cinco años, no renovable. Durante su mandato permanecerá, en su caso, en situación de servicios especiales y ejercerá exclusivamente las funciones inherentes a su cargo. Sólo podrá ser cesada por incapacidad o incumplimiento grave de sus deberes, apreciados por el Pleno mediante mayoría absoluta.

4. El régimen de incompatibilidades de la persona titular de la Dirección de Supervisión y Control de Protección de Datos será el mismo que el establecido para los Magistrados al servicio de los órganos técnicos del Consejo General del Poder Judicial. La persona titular de la Dirección de Supervisión y Control de Protección de Datos deberá ejercer sus funciones con absoluta independencia y neutralidad.

5. La persona titular y el resto de personal adscrito a la Dirección de Supervisión y Control de Protección de Datos estarán sujetos al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus atribuciones. Este deber de secreto profesional se aplicará en particular a la información que faciliten las personas físicas a la Dirección de Supervisión y Control de Protección de Datos en materia de infracciones de la presente normativa.

6. La composición, organización y funcionamiento de la Dirección de Supervisión y Control de Protección de Datos será regulada reglamentariamente. El Consejo General del Poder Judicial deberá velar porque la Dirección cuente, en todo caso, con todos los medios personales y materiales necesarios para el adecuado ejercicio de sus funciones.»

Trece. El artículo 236 decies, queda redactado como sigue:

«Artículo 236 decies.

1. Los tratamientos de datos llevados a cabo por el Consejo General del Poder judicial y la Fiscalía General del Estado en el ejercicio de sus competencias quedarán sometidos a lo dispuesto en la legislación vigente en materia de protección de datos personales. Dichos tratamientos no serán considerados en ningún caso realizados con fines jurisdiccionales.

2. Las operaciones de tratamiento de datos personales del Consejo General del Poder Judicial y de los órganos integrantes del mismo serán autorizados por acuerdo del Consejo General del Poder Judicial, a propuesta de la Secretaría General, que ostentará la condición de responsable del tratamiento respecto de los mismos.

3. Las operaciones de tratamiento de datos personales de la Fiscalía General del Estado serán autorizadas según determine el Estatuto Orgánico del Ministerio Fiscal y las Instrucciones que se dicten al respecto.»

Catorce. El ordinal 19.º del apartado 1 del artículo 560 queda redactado como sigue:

«Artículo 560.

1.º (…)
19.º En materia de protección de datos personales, ejercerá las funciones definidas en el artículo 236 octies.»

Disposición final cuarta. *Modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

Uno. Se incluye un nuevo apartado 5 en el artículo 2 con la siguiente redacción:

«Artículo 2.

5. El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables.»

Dos. Se modifica el apartado 3 del artículo 44, que queda redactado como sigue:

«Artículo 44.

3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.»

Tres. Se modifica la disposición adicional decimoquinta que queda redactada como sigue:

«Disposición adicional decimoquinta. *Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores.*

Cuando no haya podido obtener por otros medios la información necesaria para realizar sus labores de supervisión e inspección relacionadas con la detección de delitos graves, la Comisión Nacional del Mercado de Valores podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, los datos que obren en su poder relativos a la comunicación electrónica o servicio de la sociedad de la información proporcionados por dichos prestadores que sean distintos a su contenido y resulten imprescindibles para el ejercicio de dichas labores.

La cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales.»

Disposición final quinta. *Modificación de la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.*

Se modifica el artículo 10 que queda redactado como sigue:

«1. Los momentos en los que las compañías aéreas deben transmitir los datos PNR a la UIP serán los siguientes:

a) Entre las 24 y las 48 horas antes de la hora de salida programada del vuelo, e

b) inmediatamente después del cierre del vuelo, una vez que los pasajeros hayan embarcado en el avión en preparación de la salida y no sea posible embarcar o desembarcar.

Las compañías aéreas podrán limitar esta transmisión prevista en el párrafo b) a las actualizaciones de la información transmitida conforme al párrafo a).

2. El Proveedor de Servicios de Navegación Aérea en el espacio aéreo de soberanía española, comunicará a la UIP los cambios de destino, así como las escalas no programadas que le sean notificados por la tripulación de la aeronave o por otro Proveedor de Servicios de Navegación Aérea».

3. Además, cuando sea necesario acceder a los datos PNR para responder a una amenaza real y concreta relacionada con delitos de terrorismo o con delitos graves, en momentos distintos de los previstos en el apartado 1, todos los sujetos obligados, caso por caso, deberán transmitir a la UIP dichos datos con carácter inmediato al requerimiento recibido.»

Disposición final sexta. *Modificación de la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.*

Se modifica el artículo 30 que queda redactado como sigue:

«Artículo 30. *Procedimiento sancionador.*

1. El ejercicio de la potestad sancionadora a la que se refiere este título, se regirá por lo dispuesto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y sus disposiciones de desarrollo, sin perjuicio de las especialidades que se regulan en este título.

2. El procedimiento caducará transcurridos seis meses desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concurra identidad de sujeto, hecho y fundamento, hasta la finalización de éste.»

Disposición final séptima. *Modificación de la Ley 5/2014, de 4 de abril, de Seguridad Privada.*

Se modifica el artículo 69 que queda redactado como sigue:

«Artículo 69. *Régimen Jurídico.*

1. El ejercicio de la potestad sancionadora en materia de seguridad privada se regirá por lo dispuesto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y sus disposiciones de desarrollo, sin perjuicio de las especialidades que se regulan en este título.

2. El procedimiento caducará transcurridos seis meses desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concurra identidad de sujeto, hecho y fundamento, hasta la finalización de éste.

3. Iniciado el procedimiento sancionador, el órgano que haya ordenado su incoación podrá adoptar las medidas cautelares necesarias para garantizar su adecuada instrucción, así como para evitar la continuación de la infracción o asegurar el pago de la sanción, en el caso de que ésta fuese pecuniaria, y el cumplimiento de la misma en los demás supuestos.

4. Dichas medidas, que deberán ser congruentes con la naturaleza de la presunta infracción y proporcionadas a la gravedad de la misma, podrán consistir en:

a) La ocupación o precinto de vehículos, armas, material o equipo prohibido, no homologado o que resulte peligroso o perjudicial, así como de los instrumentos y efectos de la infracción.

b) La retirada preventiva de las autorizaciones, habilitaciones, permisos o licencias, o la suspensión, en su caso, de la eficacia de las declaraciones responsables.

c) La suspensión de la habilitación del personal de seguridad privada y, en su caso, de la tramitación del procedimiento para el otorgamiento de aquélla, mientras dure la instrucción de expedientes por infracciones graves o muy graves en materia de seguridad privada.

También podrán ser suspendidas las indicadas habilitación y tramitación, hasta tanto finalice el proceso por delitos contra dicho personal.

5. Las medidas cautelares previstas en los párrafos b) y c) del apartado anterior no podrán tener una duración superior a un año.»

Disposición final octava. *Modificación del texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 6/2015, de 30 de octubre.*

Se modifica el artículo 68 que queda redactado como sigue:

«Artículo 68. *Matrículas.*

1. Para poner en circulación vehículos a motor, así como remolques de masa máxima autorizada superior a la que reglamentariamente se determine, es preciso matricularlos y que lleven las placas de matrícula con los caracteres que se les asigne del modo que se establezca. Esta obligación será exigida a los ciclomotores en los términos que reglamentariamente se determine.

2. Deben ser objeto de matriculación definitiva en España los vehículos a los que se refiere el apartado anterior, cuando se destinen a ser utilizados en el territorio español por personas o entidades que sean residentes en España o que sean titulares de establecimientos situados en España. Reglamentariamente se establecerán los plazos, requisitos y condiciones para el cumplimiento de esta obligación y las posibles exenciones a la misma.

3. La matriculación ordinaria será única para cada vehículo, salvo en los supuestos que se determinen reglamentariamente. Cuando concurran circunstancias que puedan afectar a la Seguridad Nacional, el Secretario de Estado de Seguridad podrá autorizar una nueva matrícula distinta de la inicialmente asignada. Este tipo de matrículas no serán públicas en el Registro General de Vehículos e, incluso en circunstancias excepcionales, podrá utilizarse una titularidad supuesta en el marco de la actuación de las Fuerzas y Cuerpos de Seguridad y del Centro Nacional de Inteligencia en el tráfico jurídico.

4. En casos justificados, la autoridad competente para expedir el permiso de circulación podrá conceder permisos de circulación temporales y provisionales en los términos que se determine reglamentariamente.»

Disposición final novena. *Naturaleza de la ley.*

Esta ley tiene el carácter de Ley Orgánica. No obstante, tienen carácter ordinario:

a) El capítulo VI.
b) El capítulo VII.
c) El capítulo VIII.
d) Las disposiciones finales segunda, sexta, séptima y octava.

Disposición final décima. *Título competencial.*

Esta Ley Orgánica se dicta al amparo de las reglas 1.ª, 6.ª, 18.ª y 29.ª del artículo 149.1 de la Constitución, que atribuyen al Estado las competencias exclusivas, respectivamente, para la regulación de las condiciones básicas que garanticen la igualdad de todos los

españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales; respecto a las bases del régimen jurídico de las Administraciones Públicas, el procedimiento administrativo común y en relación al sistema de responsabilidad de todas las Administraciones públicas; sobre legislación penal, penitenciaria, procesal; y en materia de seguridad pública.

Disposición final undécima. *Incorporación del Derecho de la Unión Europea.*

Mediante esta Ley Orgánica se incorpora al ordenamiento jurídico español la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Disposición final duodécima. *Entrada en vigor.*

Esta Ley Orgánica entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

No obstante, las previsiones contenidas en el capítulo IV producirán efectos a los seis meses de la entrada en vigor de la Ley Orgánica.

§ 5

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Ministerio de Justicia
«BOE» núm. 17, de 19 de enero de 2008
Última modificación: 8 de marzo de 2012
Referencia: BOE-A-2008-979

La actual Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal adaptó nuestro ordenamiento a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal.

La nueva ley, que ha nacido con una amplia vocación de generalidad, prevé en su artículo 1 que «tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal». Comprende por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal.

A fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos, el legislador declaró subsistentes las normas reglamentarias existentes y, en especial, los reales decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999.

Por otra parte, la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones atribuyen competencias en materia sancionadora a la Agencia Española de Protección de Datos. Éstas requieren de desarrollo reglamentario con la peculiaridad de que ambas normas se ordenan a la tutela no sólo de los derechos de las personas físicas, sino también de las jurídicas.

II

Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo.

Por tanto, se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema.

III

El reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia.

El reglamento se estructura en nueve títulos cuyo contenido desarrolla los aspectos esenciales en esta materia.

El título I contempla el objeto y ámbito de aplicación del reglamento. A lo largo de la vigencia de la Ley Orgánica 15/1999, se ha advertido la conveniencia de desarrollar el apartado 2 de su artículo 2 para aclarar qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que están excluidos de la normativa sobre protección de datos de carácter personal.

Por otra parte, el presente reglamento no contiene previsiones para los tratamientos de datos personales a los que se refiere el apartado 3 del artículo 2 de la ley orgánica, dado que se rigen por sus disposiciones específicas y por lo especialmente previsto, en su caso, por la propia Ley Orgánica 15/1999. En consecuencia, se mantiene el régimen jurídico propio de estos tratamientos y ficheros.

Además, en este título se aporta un conjunto de definiciones que ayudan al correcto entendimiento de la norma, lo que resulta particularmente necesario en un ámbito tan tecnificado como el de la protección de datos personales. Por otra parte, fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.

El título II, se refiere a los principios de la protección de datos. Reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de los servicios de comunicaciones electrónicas y, muy particularmente, la captación de datos de los menores. Asimismo, se ofrece lo que no puede definirse sino como un estatuto del encargado del tratamiento, que sin duda contribuirá a clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de una cuestión tan esencial como los derechos de las personas en este ámbito. Estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

A continuación, los títulos IV a VII permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían -los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial-, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, finalmente, la regulación de un instrumento, el código tipo, llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos.

El título VIII regula un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. La repercusión del deber de seguridad obligaba a un particular rigor ya que en esta materia han confluido distintos elementos muy relevantes. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la regulación. Por otra, se reclamaba la adaptación de la regulación en distintos aspectos. En este sentido, el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica. Por último, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al presente reglamento.

En su virtud, a propuesta del Ministro de Justicia, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 21 de diciembre de 2007.

D I S P O N G O :

Artículo único. *Aprobación del reglamento.*

Se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Adaptación de los códigos tipo inscritos en el Registro General de Protección de Datos.*

En el plazo de un año desde la entrada en vigor del presente real decreto deberán notificarse a la Agencia Española de Protección de Datos las modificaciones que resulten necesarias en los códigos tipo inscritos en el Registro General de Protección de Datos para adaptar su contenido a lo dispuesto en el título VII del mismo.

Disposición transitoria segunda. *Plazos de implantación de las medidas de seguridad.*

La implantación de las medidas de seguridad previstas en el presente real decreto deberá producirse con arreglo a las siguientes reglas:

1.ª Respecto de los ficheros automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) En el plazo de un año desde su entrada en vigor, deberán implantarse las medidas de seguridad de nivel medio exigibles a los siguientes ficheros:

1.º Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.

2.º Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

3.º Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

b) En el plazo de un año desde su entrada en vigor deberán implantarse las medidas de seguridad de nivel medio y en el de dieciocho meses desde aquella fecha, las de nivel alto exigibles a los siguientes ficheros:

1.º Aquéllos que contengan datos derivados de actos de violencia de género.

2.º Aquéllos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

c) En los demás supuestos, cuando el presente reglamento exija la implantación de una medida adicional, no prevista en el Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, dicha medida deberá implantarse en el plazo de un año desde la entrada en vigor del presente real decreto.

2.ª Respecto de los ficheros no automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) Las medidas de seguridad de nivel básico deberán implantarse en el plazo de un año desde su entrada en vigor.

b) Las medidas de seguridad de nivel medio deberán implantarse en el plazo de dieciocho meses desde su entrada en vigor.

c) Las medidas de seguridad de nivel alto deberán implantarse en el plazo de dos años desde su entrada en vigor.

3.ª Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del presente real decreto deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

Disposición transitoria tercera. *Régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas.*

A las solicitudes para el ejercicio de los derechos de acceso, oposición, rectificación y cancelación que hayan sido efectuadas antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria cuarta. *Régimen transitorio de los procedimientos.*

A los procedimientos ya iniciados antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria quinta. *Régimen transitorio de las actuaciones previas.*

A las actuaciones previas iniciadas con anterioridad a la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

El presente real decreto se aplicará a las actuaciones previas que se inicien después de su entrada en vigor.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogados el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del

tratamiento automatizado de los datos de carácter personal, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en el presente real decreto.

Disposición final primera. *Título competencial.*

El título I, con excepción del apartado c) del artículo 4, los títulos II, III, VII y VIII, así como los artículos 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 y 63.3 del reglamento se dictan al amparo de lo dispuesto en el artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor a los tres meses de su íntegra publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

2. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 2. *Ámbito objetivo de aplicación.*

1. El presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

4. Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Artículo 3. *Ámbito territorial de aplicación.*

1. Se regirá por el presente reglamento todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.

Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española, según las normas de Derecho internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

2. A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Artículo 4. *Ficheros o tratamientos excluidos.*

El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:

a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

b) A los sometidos a la normativa sobre protección de materias clasificadas.

c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Artículo 5. *Definiciones.*

1. A los efectos previstos en este reglamento, se entenderá por:

a) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

b) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

c) Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

d) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

e) Dato disociado: aquél que no permite la identificación de un afectado o interesado.

f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

g) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

h) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

i) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

j) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

k) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

l) Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

ñ) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

p) Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

r) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien

constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

t) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

2. En particular, en relación con lo dispuesto en el título VIII de este reglamento se entenderá por:

a) Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

b) Autenticación: procedimiento de comprobación de la identidad de un usuario.

c) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

d) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

e) Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

f) Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

g) Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

h) Identificación: procedimiento de reconocimiento de la identidad de un usuario.

i) Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

j) Perfil de usuario: accesos autorizados a un grupo de usuarios.

k) Recurso: cualquier parte componente de un sistema de información.

l) Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

m) Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

n) Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

ñ) Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

o) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

p) Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Artículo 6. *Cómputo de plazos.*

En los supuestos en que este reglamento señale un plazo por días se computarán únicamente los hábiles. Cuando el plazo sea por meses, se computarán de fecha a fecha.

Artículo 7. *Fuentes accesibles al público.*

1. A efectos del artículo 3, párrafo j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:

a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.

c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los diarios y boletines oficiales.

e) Los medios de comunicación social.

2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

TÍTULO II

Principios de protección de datos

CAPÍTULO I

Calidad de los datos

Artículo 8. *Principios relativos a la calidad de los datos.*

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.

6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 9. *Tratamiento con fines estadísticos, históricos o científicos.*

1. No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

2. Por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

Artículo 10. *Supuestos que legitiman el tratamiento o cesión de los datos.*

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) **(Anulado)**

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Artículo 11. *Verificación de datos en solicitudes formuladas a las Administraciones públicas.*

(Anulado)

CAPÍTULO II

Consentimiento para el tratamiento de los datos y deber de información

Sección 1.ª Obtención del consentimiento del afectado

Artículo 12. *Principios generales.*

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Artículo 13. *Consentimiento para el tratamiento de datos de menores de edad.*

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos.

No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Artículo 14. *Forma de recabar el consentimiento.*

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. *Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.*

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 16. *Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.*

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. *Revocación del consentimiento.*

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

Sección 2.ª Deber de información al interesado

Artículo 18. *Acreditación del cumplimiento del deber de información.*

(Anulado)

Artículo 19. *Supuestos especiales.*

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Encargado del tratamiento

Artículo 20. *Relaciones entre el responsable y el encargado del tratamiento.*

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. *Posibilidad de subcontratación de los servicios.*

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. *Conservación de los datos por el encargado del tratamiento.*

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

TÍTULO III

Derechos de acceso, rectificación, cancelación y oposición

CAPÍTULO I

Disposiciones generales

Artículo 23. *Carácter personalísimo.*

1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.

2. Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.

b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

Artículo 24. *Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Artículo 25. *Procedimiento.*

1. Salvo en el supuesto referido en el párrafo 4 del artículo anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

2. El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

3. En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

4. La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.

5. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.

6. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

7. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las Leyes.

8. Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas.

Artículo 26. *Ejercicio de los derechos ante un encargado del tratamiento.*

Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

CAPÍTULO II

Derecho de acceso

Artículo 27. *Derecho de acceso.*

1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

2. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.

No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.

3. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 28. *Ejercicio del derecho de acceso.*

1. Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

a) Visualización en pantalla.
b) Escrito, copia o fotocopia remitida por correo, certificado o no.
c) Telecopia.
d) Correo electrónico u otros sistemas de comunicaciones electrónicas.
e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

2. Los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige.
3. El responsable del fichero deberá cumplir al facilitar el acceso lo establecido en el Título VIII de este Reglamento.

Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.
Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.

Artículo 29. *Otorgamiento del acceso.*

1. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.
En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.
2. Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que se refiere el artículo 27.1, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.
3. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Artículo 30. *Denegación del acceso.*

1. El responsable del fichero o tratamiento podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.
2. Podrá también denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.
3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Derechos de rectificación y cancelación

Artículo 31. *Derechos de rectificación y cancelación.*

1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.

En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento.

Artículo 32. *Ejercicio de los derechos de rectificación y cancelación.*

1. La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

2. El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 33. *Denegación de los derechos de rectificación y cancelación.*

1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

2. Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO IV

Derecho de oposición

Artículo 34. *Derecho de oposición.*

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento.

Artículo 35. *Ejercicio del derecho de oposición.*

1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

2. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo.

Artículo 36. *Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.*

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

TÍTULO IV

Disposiciones aplicables a determinados ficheros de titularidad privada

CAPÍTULO I

Ficheros de información sobre solvencia patrimonial y crédito

Sección 1.ª Disposiciones generales

Artículo 37. *Régimen aplicable.*

1. El tratamiento de datos de carácter personal sobre solvencia patrimonial y crédito, previsto en el apartado 1 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, se

someterá a lo establecido, con carácter general, en dicha ley orgánica y en el presente reglamento.

2. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros a que se refiere el apartado anterior, se rige por lo dispuesto en los capítulos I a IV del título III del presente reglamento, con los siguientes criterios:

a) Cuando la petición de ejercicio de los derechos se dirigiera al responsable del fichero, éste estará obligado a satisfacer, en cualquier caso, dichos derechos.

b) Si la petición se dirigiera a las personas y entidades a las que se presta el servicio, éstas únicamente deberán comunicar al afectado aquellos datos relativos al mismo que les hayan sido comunicados y a facilitar la identidad del responsable para que, en su caso, puedan ejercitar sus derechos ante el mismo.

3. De conformidad con el apartado 2 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, también podrán tratarse los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

Estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado y su tratamiento se regirá por lo dispuesto en el presente reglamento y, en particular, por las previsiones contenidas en la sección segunda de este capítulo.

Sección 2.ª Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés

Artículo 38. *Requisitos para la inclusión de los datos.*

1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada **y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.**

> Téngase en cuenta que se anula el inciso destacado de la letra a) del apartado 1 por Sentencias del TS de 15 de julio de 2010. Ref. BOE-A-2010-16299 y Ref. BOE-A-2010-16301

b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

2. **(Anulado)**

3. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo siguiente.

Artículo 39. *Información previa a la inclusión.*

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento al que se refiere la letra c) del apartado 1 del artículo anterior, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos en el citado artículo, los datos relativos al impago podrán

ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Artículo 40. *Notificación de inclusión.*

1. El responsable del fichero común deberá notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos, informándole asimismo de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre.

2. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

3. La notificación deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos.

4. En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

No se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

5. Si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato.

Artículo 41. *Conservación de los datos.*

1. Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.

El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma.

2. En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

Artículo 42. *Acceso a la información contenida en el fichero.*

1. Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

a) Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.

b) Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.

c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

2. Los terceros deberán informar por escrito a las personas en las que concurran los supuestos contemplados en las letras b) y c) precedentes de su derecho a consultar el fichero.

En los supuestos de contratación telefónica de los productos o servicios a los que se refiere el párrafo anterior, la información podrá realizarse de forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar.

Artículo 43. *Responsabilidad.*

1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.

2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 44. *Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición se rige por lo dispuesto en los capítulos I a IV del título III de este reglamento, sin perjuicio de lo señalado en el presente artículo.

2. Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.

En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

2.ª Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

3. Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.

2.ª Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días, dando asimismo respuesta al interesado en los términos previstos en el artículo 33 de este reglamento.

3.ª Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad y dirección del titular del fichero común para, que en su caso, puedan ejercitar sus derechos ante el mismo.

CAPÍTULO II

Tratamientos para actividades de publicidad y prospección comercial

Artículo 45. *Datos susceptibles de tratamiento e información al interesado.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros, sólo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:

a) Figuren en alguna de las fuentes accesibles al público a las que se refiere la letra j) del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre y el artículo 7 de este

reglamento y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas en este apartado.

b) Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

2. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.

Artículo 46. *Tratamiento de datos en campañas publicitarias.*

1. Para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes será preciso que el tratamiento se ampare en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre.

2. En caso de que una entidad contrate o encomiende a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas:

a) Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.

b) Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.

c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

3. En el supuesto contemplado en el apartado anterior, la entidad que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

4. A los efectos previstos en este artículo, se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

Artículo 47. *Depuración de datos personales.*

Cuando dos o más responsables por sí mismos o mediante encargo a terceros pretendieran constatar sin consentimiento de los afectados, con fines de promoción o comercialización de sus productos o servicios y mediante un tratamiento cruzado de sus ficheros quiénes ostentan la condición de clientes de una u otra o de varios de ellos, el tratamiento así realizado constituirá una cesión o comunicación de datos.

Artículo 48. *Ficheros de exclusión del envío de comunicaciones comerciales.*

Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Artículo 49. *Ficheros comunes de exclusión del envío de comunicaciones comerciales.*

1. Será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para

evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

2. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

3. La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.

4. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Artículo 50. *Derechos de acceso, rectificación y cancelación.*

1. El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial se someterá a lo previsto en los capítulos I a IV del título III de este reglamento.

2. Si el derecho se ejercitase ante una entidad que hubiese encargado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo otorgue al afectado su derecho en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 51. *Derecho de oposición.*

1. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

La oposición a la que se refiere el párrafo anterior deberá entenderse sin perjuicio del derecho del interesado a revocar cuando lo estimase oportuno el consentimiento que hubiera otorgado, en su caso, para el tratamiento de los datos.

2. A tal efecto, deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento. En particular, se considerará cumplido lo dispuesto en este precepto cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico.

3. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar su oposición el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

En todo caso, el ejercicio por el afectado de sus derechos no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

4. Si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo atienda el derecho del afectado en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

TÍTULO V

Obligaciones previas al tratamiento de los datos

CAPÍTULO I

Creación, modificación o supresión de ficheros de titularidad pública

Artículo 52. *Disposición o Acuerdo de creación, modificación o supresión del fichero.*

1. La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente.

2. En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero.

Artículo 53. *Forma de la disposición o acuerdo.*

1. Cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

2. En el caso de los órganos constitucionales del Estado, se estará a lo que establezcan sus normas reguladoras.

3. En relación con los ficheros de los que sean responsables las comunidades autónomas, entidades locales y las entidades u organismos vinculados o dependientes de las mismas, las universidades públicas, así como los órganos de las comunidades autónomas con funciones análogas a los órganos constitucionales del Estado, se estará a su legislación específica.

4. La creación, modificación o supresión de los ficheros de los que sean responsables las corporaciones de derecho público y que se encuentren relacionados con el ejercicio por aquéllas de potestades de derecho público deberá efectuarse a través de acuerdo de sus órganos de gobierno, en los términos que establezcan sus respectivos Estatutos, debiendo ser igualmente objeto de publicación en el «Boletín Oficial del Estado» o diario oficial correspondiente.

Artículo 54. *Contenido de la disposición o acuerdo.*

1. La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.

b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.

c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.

e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.

f) Los órganos responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

2. La disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los extremos a los que se refiere el apartado anterior.

3. En las disposiciones o acuerdos que se dicten para la supresión de los ficheros se establecerá el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

CAPÍTULO II

Notificación e inscripción de los ficheros de titularidad pública o privada

Artículo 55. *Notificación de ficheros.*

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.

El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las comunidades autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.

4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Artículo 56. *Tratamiento de datos en distintos soportes.*

1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.

2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.

Artículo 57. *Ficheros en los que exista más de un responsable.*

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.

Artículo 58. *Notificación de la modificación o supresión de ficheros.*

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

3. Tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título.

Artículo 59. *Modelos y soportes para la notificación.*

1. La Agencia Española de Protección de Datos publicará mediante la correspondiente Resolución del Director los modelos o formularios electrónicos de notificación de creación, modificación o supresión de ficheros, que permitan su presentación a través de medios telemáticos o en soporte papel, así como, previa consulta de las autoridades de protección de datos de las comunidades autónomas, los formatos para la comunicación telemática de ficheros públicos por las autoridades de control autonómicas, de conformidad con lo establecido en los artículos 55 y 58 del presente reglamento.

2. Los modelos o formularios electrónicos de notificación se podrán obtener gratuitamente en la página web de la Agencia Española de Protección de Datos.

3. El Director de la Agencia Española de Protección de Datos podrá establecer procedimientos simplificados de notificación en atención a las circunstancias que concurran en el tratamiento o el tipo de fichero al que se refiera la notificación.

Artículo 60. *Inscripción de los ficheros.*

1. El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando, en su caso, la inscripción, una vez tramitado el procedimiento previsto en el capítulo IV del título IX.

2. La inscripción contendrá el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad exigible conforme a lo dispuesto en el artículo 81.

Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales.

En el caso de ficheros de titularidad pública también se hará constar la referencia de la disposición general por la que ha sido creado, y en su caso, modificado.

3. La inscripción de un fichero en el Registro General de Protección de Datos, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la Ley Orgánica 15/1999, de 13 de diciembre, y demás disposiciones reglamentarias.

Artículo 61. *Cancelación de la inscripción.*

1. Cuando el responsable del tratamiento comunicase, en virtud de lo dispuesto en el artículo 58 de este reglamento, la supresión del fichero, el Director de la Agencia Española de Protección de Datos, previa la tramitación del procedimiento establecido en la sección primera del capítulo IV del título IX, dictará resolución acordando la cancelación de la inscripción correspondiente al fichero.

2. El Director de la Agencia Española de Protección de Datos podrá, en ejercicio de sus competencias, acordar de oficio la cancelación de la inscripción de un fichero cuando concurran circunstancias que acrediten la imposibilidad de su existencia, previa la tramitación del procedimiento establecido en la sección segunda del capítulo IV del título IX de este reglamento.

Artículo 62. *Rectificación de errores.*

El Registro General de Protección de Datos podrá rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos que pudieran existir en las inscripciones, de conformidad con lo dispuesto en el artículo 105 de la Ley 30/1992, de 26 de noviembre.

Artículo 63. *Inscripción de oficio de ficheros de titularidad pública.*

1. En supuestos excepcionales con el fin de garantizar el derecho a la protección de datos de los afectados, y sin perjuicio de la obligación de notificación, se podrá proceder a la inscripción de oficio de un determinado fichero en el Registro General de Protección de Datos.

2. Para que lo dispuesto en el apartado anterior resulte de aplicación, será requisito indispensable que la correspondiente norma o acuerdo regulador de los ficheros que contengan datos de carácter personal haya sido publicado en el correspondiente diario oficial y cumpla los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

3. El Director de la Agencia Española de Protección de Datos podrá, a propuesta del Registro General de Protección de Datos, acordar la inscripción del fichero de titularidad pública en el Registro, notificándose dicho acuerdo al órgano responsable del fichero.

Cuando la inscripción se refiera a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, se comunicará a la referida autoridad de control autonómica para que proceda, en su caso, a la inscripción de oficio.

Artículo 64. *Colaboración con las autoridades de control de las comunidades autónomas.*

El Director de la Agencia Española de Protección de Datos podrá celebrar con los directores de las autoridades de control de las comunidades autónomas los convenios de colaboración o acuerdos que estime pertinentes, a fin de garantizar la inscripción en el Registro General de Protección de Datos de los ficheros sometidos a la competencia de dichas autoridades autonómicas.

TÍTULO VI

Transferencias internacionales de datos

CAPÍTULO I

Disposiciones generales

Artículo 65. *Cumplimiento de las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre.*

La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

Artículo 66. *Autorización y notificación.*

1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento.

La autorización se otorgará conforme al procedimiento establecido en la sección primera del capítulo V del título IX de este reglamento.

2. La autorización no será necesaria:

a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II de este título.

b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

CAPÍTULO II

Transferencias a estados que proporcionen un nivel adecuado de protección

Artículo 67. *Nivel adecuado de protección acordado por la Agencia Española de Protección de Datos.*

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el «Boletín Oficial del Estado».

2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior.

Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos.

Artículo 68. *Nivel adecuado de protección declarado por Decisión de la Comisión Europea.*

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

Artículo 69. *Suspensión temporal de las transferencias.*

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea.

CAPÍTULO III

Transferencias a Estados que no proporcionen un nivel adecuado de protección

Artículo 70. *Transferencias sujetas a autorización del Director de la Agencia Española de Protección de Datos.*

1. Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

La autorización de la transferencia se tramitará conforme al procedimiento establecido en la sección primera del capítulo V del título IX del presente reglamento.

2. La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de

diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

3. En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

4. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.

En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

TÍTULO VII

Códigos tipo

Artículo 71. *Objeto y naturaleza.*

1. Los códigos tipo a los que se refiere el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, tienen por objeto adecuar lo establecido en la citada Ley Orgánica y en el presente reglamento a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Artículo 72. *Iniciativa y ámbito de aplicación.*

1. Los códigos tipo tendrán carácter voluntario.

2. Los códigos tipo de carácter sectorial podrán referirse a la totalidad o a parte de los tratamientos llevados a cabo por entidades pertenecientes a un mismo sector, debiendo ser formulados por organizaciones representativas de dicho sector, al menos en su ámbito territorial de aplicación, y sin perjuicio de la potestad de dichas entidades de ajustar el código tipo a sus peculiaridades.

3. Los códigos tipo promovidos por una empresa deberán referirse a la totalidad de los tratamientos llevados a cabo por la misma.

4. Las Administraciones públicas y las corporaciones de Derecho Público podrán adoptar códigos tipo de acuerdo con lo establecido en las normas que les sean aplicables.

Artículo 73. *Contenido.*

1. Los códigos tipo deberán estar redactados en términos claros y accesibles.

2. Los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión:

a) La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.

b) Las previsiones específicas para la aplicación de los principios de protección de datos.

c) El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.

d) El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

e) La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.

f) Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.

g) Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo, en los términos previstos en el artículo 74 de este reglamento.

3. En particular, deberán contenerse en el código:

a) Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.

b) Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.

c) Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

d) Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Artículo 74. *Compromisos adicionales.*

1. Los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos.

2. Además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras y, en particular, sobre:

a) La adopción de medidas de seguridad adicionales a las exigidas por la Ley Orgánica 15/1999, de 13 de diciembre, y el presente Reglamento.

b) La identificación de las categorías de cesionarios o importadores de los datos.

c) Las medidas concretas adoptadas en materia de protección de los menores o de determinados colectivos de afectados.

d) El establecimiento de un sello de calidad que identifique a los adheridos al código.

Artículo 75. *Garantías del cumplimiento de los códigos tipo.*

1. Los códigos tipo deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

2. El procedimiento que se prevea deberá garantizar:

a) La independencia e imparcialidad del órgano responsable de la supervisión.

b) La sencillez, accesibilidad, celeridad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código tipo.

c) El principio de contradicción.

d) Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias y podrán implicar la suspensión de la adhesión al código o la expulsión de la entidad adherida. Asimismo, podrá establecerse, en su caso, su publicidad.

e) La notificación al afectado de la decisión adoptada.

3. Asimismo, y sin perjuicio de lo dispuesto en el artículo 19 de la Ley Orgánica 15/1999, de 13 de diciembre, los códigos tipo podrán contemplar procedimientos para la determinación de medidas reparadoras en caso de haberse causado un perjuicio a los afectados como consecuencia del incumplimiento del código tipo.

4. Lo dispuesto en este artículo se aplicará sin perjuicio de las competencias de la Agencia Española de Protección de Datos y, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 76. *Relación de adheridos.*

El código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la Agencia Española de Protección de Datos.

Artículo 77. *Depósito y publicidad de los códigos tipo.*

1. Para que los códigos tipo puedan ser considerados como tales a los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento, deberán ser depositados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al Registro General de Protección de Datos.

2. A tal efecto, los códigos tipo deberán ser presentados ante la correspondiente autoridad de control, tramitándose su inscripción, en caso de estar sometidos a la decisión de la Agencia Española de Protección de Datos, conforme al procedimiento establecido en el capítulo VI del título IX de este reglamento.

3. En todo caso, la Agencia Española de Protección de Datos dará publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos.

Artículo 78. *Obligaciones posteriores a la inscripción del código tipo.*

Las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el propio código tipo tendrán, una vez el mismo haya sido publicado, las siguientes obligaciones:

a) Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior.

Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

b) Remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar.

Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al registro General de Protección de Datos.

c) Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

d) Favorecer la accesibilidad de todas las personas, con especial atención a las que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo.

TÍTULO VIII

De las medidas de seguridad en el tratamiento de datos de carácter personal

CAPÍTULO I

Disposiciones generales

Artículo 79. *Alcance.*

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. *Niveles de seguridad.*

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. *Aplicación de los niveles de seguridad.*

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. *Encargado del tratamiento.*

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. *Prestaciones de servicios sin acceso a datos personales.*

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos

del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 84. *Delegación de autorizaciones.*

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. *Acceso a datos a través de redes de comunicaciones.*

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. *Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.*

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. *Ficheros temporales o copias de trabajo de documentos.*

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II

Del documento de seguridad

Artículo 88. *El documento de seguridad.*

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPÍTULO III

Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 89. *Funciones y obligaciones del personal.*

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. *Registro de incidencias.*

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. *Control de acceso.*

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. *Gestión de soportes y documentos.*

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.
3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. *Identificación y autenticación.*

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. *Copias de respaldo y recuperación.*

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 95. *Responsable de seguridad.*

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. *Auditoría.*

1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. *Gestión de soportes y documentos.*

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. *Identificación y autenticación.*

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. *Control de acceso físico.*

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. *Registro de incidencias.*

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 101. *Gestión y distribución de soportes.*

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. *Copias de respaldo y recuperación.*

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos

informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. *Registro de accesos.*

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. *Telecomunicaciones.*

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO IV

Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 105. *Obligaciones comunes.*

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
a) Funciones y obligaciones del personal.

b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. *Criterios de archivo.*

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. *Dispositivos de almacenamiento.*

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. *Custodia de los soportes.*

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 109. *Responsable de seguridad.*

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. *Auditoría.*

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 111. *Almacenamiento de la información.*

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. *Copia o reproducción.*

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. *Acceso a la documentación.*

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. *Traslado de documentación.*

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

TÍTULO IX

Procedimientos tramitados por la Agencia Española de Protección de Datos

CAPÍTULO I

Disposiciones generales

Artículo 115. *Régimen aplicable.*

1. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el presente título, y supletoriamente, por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. Específicamente serán de aplicación las normas reguladoras del procedimiento administrativo común al régimen de representación en los citados procedimientos.

Artículo 116. *Publicidad de las resoluciones.*

1. La Agencia Española de Protección de Datos hará públicas sus resoluciones, con excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo, siempre que se refieran a procedimientos que se hubieran iniciado con posterioridad al 1 de enero de 2004, o correspondan al archivo de actuaciones inspectoras incoadas a partir de dicha fecha.

2. La publicación de estas resoluciones se realizará preferentemente mediante su inserción en el sitio web de la Agencia Española de Protección de Datos, dentro del plazo de un mes a contar desde la fecha de su notificación a los interesados.

3. En la notificación de las resoluciones se informará expresamente a los interesados de la publicidad prevista en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. La publicación se realizará aplicando los criterios de disociación de los datos de carácter personal que a tal efecto se establezcan mediante Resolución del Director de la Agencia.

CAPÍTULO II

Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición

Artículo 117. *Instrucción del procedimiento.*

1. El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, que se consideran vulnerados.

2. Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

3. Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

Artículo 118. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la reclamación del afectado o afectados.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su reclamación por silencio administrativo positivo.

Artículo 119. *Ejecución de la resolución.*

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo.

CAPÍTULO III

Procedimientos relativos al ejercicio de la potestad sancionadora

Sección 1.ª Disposiciones generales

Artículo 120. *Ámbito de aplicación.*

1. Las disposiciones contenidas en el presente capítulo serán de aplicación a los procedimientos relativos al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora que le viene atribuida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. No obstante, las disposiciones previstas en el ar-tículo 121 y en la sección cuarta de este capítulo únicamente serán aplicables a los procedimientos referidos al ejercicio de la potestad sancionadora prevista en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 121. *Inmovilización de ficheros.*

1. En el supuesto previsto como infracción muy grave en la Ley Orgánica 15/1999, de 13 de diciembre, consistente en la utilización o cesión ilícita de los datos de carácter personal en la que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, en cualquier momento del procedimiento, requerir a los responsables de ficheros o tratamientos de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos.

2. El requerimiento deberá ser atendido en el plazo improrrogable de tres días, durante el cual el responsable del fichero podrá formular las alegaciones que tenga por convenientes en orden al levantamiento de la medida.

3. Si el requerimiento fuera desatendido, el Director de la Agencia Española de Protección de Datos podrá, mediante resolución motivada, acordar la inmovilización de tales ficheros o tratamientos, a los solos efectos de restaurar los derechos de las personas afectadas.

Sección 2.ª Actuaciones previas

Artículo 122. *Iniciación.*

1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas.

Artículo 123. *Personal competente para la realización de las actuaciones previas.*

1. Las actuaciones previas serán llevadas a cabo por el personal del área de la Inspección de Datos habilitado para el ejercicio de funciones inspectoras.

2. **(Anulado)**

3. Los funcionarios que ejerzan la inspección a los que se refieren los dos apartados anteriores tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 124. *Obtención de información.*

Los inspectores podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal fin podrán requerir la exhibición o el envío de los documentos y datos y examinarlos en el lugar en que se encuentren depositados, como obtener copia de los mismos, inspeccionar los equipos físicos y lógicos, así como requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del fichero o ficheros sujetos a investigación, accediendo a los lugares donde se hallen instalados.

Artículo 125. *Actuaciones presenciales.*

1. En el desarrollo de las actuaciones previas se podrán realizar visitas de inspección por parte de los inspectores designados, en los locales o sede del inspeccionado, o donde se encuentren ubicados los ficheros, en su caso. A tal efecto, los inspectores habrán sido previamente autorizados por el Director de la Agencia Española de Protección de Datos.

Las inspecciones podrán realizarse en el domicilio del inspeccionado, en la sede o local concreto relacionado con el mismo o en cualquiera de sus locales, incluyendo aquéllos en que el tratamiento sea llevado a cabo por un encargado.

La autorización se limitará a indicar la habilitación del inspector autorizado y la identificación de la persona u órgano inspeccionado.

2. En el supuesto contemplado en el apartado anterior, las inspecciones concluirán con el levantamiento de la correspondiente acta, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de inspección.

3. El acta, que se emitirá por duplicado, será firmada por los inspectores actuantes y por el inspeccionado, que podrá hacer constar en la misma las alegaciones o manifestaciones que tenga por conveniente.

En caso de negativa del inspeccionado a la firma del acta, se hará constar expresamente esta circunstancia en la misma. En todo caso, la firma por el inspeccionado del acta no supondrá su conformidad, sino tan sólo la recepción de la misma.

Se entregará al inspeccionado uno de los originales del acta de inspección, incorporándose el otro a las actuaciones.

Artículo 126. *Resultado de las actuaciones previas.*

1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo.

Sección 3.ª Procedimiento sancionador

Artículo 127. *Iniciación del procedimiento.*

Con carácter específico el acuerdo de inicio del procedimiento sancionador deberá contener:

a) Identificación de la persona o personas presuntamente responsables.

b) Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.

c) Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos.

d) Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.

e) Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.

f) Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.

g) Medidas de carácter provisional que pudieran acordarse, en su caso, conforme a lo establecido en la sección primera del presente capítulo.

Artículo 128. *Plazo máximo para resolver.*

1. El plazo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación.

2. El vencimiento del citado plazo máximo, sin que se haya dictada y notificada resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones.

Sección 4.ª Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las administraciones públicas

Artículo 129. *Disposición general.*

El procedimiento por el que se declare la existencia de una infracción de la Ley Orgánica 15/1999, de 13 de diciembre, cometida por las Administraciones públicas será el establecido en la sección tercera de este capítulo.

CAPÍTULO IV

Procedimientos relacionados con la inscripción o cancelación de ficheros

Sección 1.ª Procedimiento de inscripción de la creación, modificación o supresión de ficheros

Artículo 130. *Iniciación del procedimiento.*

1. El procedimiento se iniciará como consecuencia de la notificación de la creación, modificación o supresión del fichero por el interesado o, en su caso, de la comunicación efectuada por las autoridades de control de las comunidades autónomas, a la que se refiere el presente reglamento.

2. La notificación se deberá efectuar cumplimentando los modelos o formularios electrónicos publicados al efecto por la Agencia Española de Protección de Datos, en virtud de lo dispuesto en el apartado 1 del artículo 59 de este reglamento.

Tratándose de la notificación de la modificación o supresión de un fichero, deberá indicarse en la misma el código de inscripción del fichero en el Registro General de Protección de Datos.

3. La notificación se efectuará en soporte electrónico, ya mediante comunicación electrónica a través de Internet mediante firma electrónica o en soporte informático, utilizando al efecto el programa de ayuda para la generación de notificaciones que la Agencia pondrá a disposición de los interesados de forma gratuita.

Será igualmente válida la notificación efectuada en soporte papel cuando para su cumplimentación hayan sido utilizados los modelos o formularios publicados por la Agencia.

4. En la notificación, el responsable del fichero deberá declarar un domicilio a efectos de notificaciones en el procedimiento.

Artículo 131. *Especialidades en la notificación de ficheros de titularidad pública.*

1. Cuando se trate de la notificación de ficheros de titularidad pública, deberá acompañarse a la notificación una copia de la norma o acuerdo de creación, modificación o supresión del fichero a que hace referencia el ar-tículo 52 del presente reglamento.

Cuando el diario oficial en el que se encuentre publicada la citada norma o acuerdo sea accesible a través de Internet, bastará con indicar en la notificación la dirección electrónica que permita su concreta localización.

2. Recibida la notificación, si la misma no contuviera la información preceptiva o se advirtieran defectos formales, el Registro General de Protección de Datos requerirá al responsable del fichero para que complete o subsane la notificación. El plazo para la subsanación o mejora de la solicitud será de tres meses, en el caso de que se precise la modificación de la norma o acuerdo de creación del fichero.

Artículo 132. *Acuerdo de inscripción o cancelación.*

Si la notificación referida a la creación, modificación o supresión del fichero contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará, respectivamente, la inscripción del fichero, asignando al mismo el correspondiente código de inscripción, la modificación de la inscripción del fichero o la cancelación de la inscripción correspondiente.

Artículo 133. *Improcedencia o denegación de la inscripción.*

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución denegando la inscripción, modificación o cancelación cuando de los documentos aportados por el responsable del fichero se desprenda que la notificación no resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

La resolución será debidamente motivada, con indicación expresa de las causas que impiden la inscripción, modificación o cancelación.

Artículo 134. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución acerca de la inscripción, modificación o cancelación será de un mes.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito, modificado o cancelado el fichero a todos los efectos.

Sección 2.ª Procedimiento de cancelación de oficio de ficheros inscritos

Artículo 135. *Iniciación del procedimiento.*

El procedimiento de cancelación de oficio de los ficheros inscritos en el Registro General de Protección de Datos se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia, por acuerdo del Director de la Agencia Española de Protección de Datos.

Artículo 136. *Terminación del expediente.*

La resolución, previa audiencia del interesado, acordará haber lugar o no a la cancelación del fichero.

Si la resolución acordase la cancelación del fichero, se dará traslado de la misma al Registro General de Protección de Datos, para que proceda a la cancelación.

CAPÍTULO V

Procedimientos relacionados con las transferencias internacionales de datos

Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos

Artículo 137. *Iniciación del procedimiento.*

1. El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros a las que se refiere el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, y el artículo 70 de este reglamento se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia.

2. En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:

a) La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos.

b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.

c) La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.

Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes.

Si la autorización se pretendiera fundar en lo dispuesto en el apartado 4 del artículo 70, deberán aportarse las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

Artículo 138. *Instrucción del procedimiento.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un

período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha Ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

3. Transcurrido el plazo previsto en el apartado 1, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 139. *Actos posteriores a la resolución.*

1. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la transferencia internacional de datos, se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción.

El Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional.

2. En todo caso, se dará traslado de la resolución de autorización o denegación de la autorización de la transferencia internacional de datos al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 140. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos

Artículo 141. *Iniciación.*

1. En los supuestos contemplados en el artículo 69 y en el apartado 3 del artículo 70, el Director de la Agencia Española de Protección de Datos podrá acordar la suspensión temporal de una transferencia internacional de datos.

2. En tales supuestos, el Director dictará acuerdo de inicio referido a la suspensión temporal de la transferencia. El acuerdo deberá ser motivado y fundarse en los supuestos previstos en este reglamento.

Artículo 142. *Instrucción y resolución.*

1. Se dará traslado del acuerdo al exportador, a fin de que en el plazo de quince días formule lo que a su derecho convenga.

2. Recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos.

Artículo 143. *Actos posteriores a la resolución.*

1. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el registro.

El Registro General de Protección de Datos inscribirá de oficio la suspensión temporal de la transferencia internacional.

2. En todo caso, se dará traslado de la resolución al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 144. *Levantamiento de la suspensión temporal.*

1. La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado, mediante resolución del Director de la Agencia Española de Protección de Datos, del que se dará traslado al exportador.

2. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el Registro.

El Registro General de Protección de Datos hará constar de oficio el levantamiento de la suspensión temporal de la transferencia internacional.

3. El acuerdo será notificado al exportador y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26. 3 de la Directiva 95/46/CE.

CAPÍTULO VI

Procedimiento de inscripción de códigos tipo

Artículo 145. *Iniciación del procedimiento.*

1. El procedimiento para la inscripción en el Registro General de Protección de Datos de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.

2. La solicitud, que deberá reunir los requisitos legalmente establecidos, habrá de acompañarse de los siguientes documentos:

a) Acreditación de la representación que concurra en la persona que presente la solicitud.

b) Contenido del acuerdo, convenio o decisión por la que se aprueba, en el ámbito correspondiente el contenido del código tipo presentado.

c) En caso de que el código tipo proceda de un acuerdo sectorial o una decisión de empresa certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó.

d) En el supuesto contemplado en la letra anterior, copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.

e) En caso de códigos tipo presentados por asociaciones u organizaciones de carácter sectorial, documentación relativa a su representatividad en el sector.

f) En caso de códigos tipo basados en decisiones de empresa, descripción de los tratamientos a los que se refiere el código tipo.

g) Código tipo sometido a la Agencia Española de Protección de Datos.

Artículo 146. *Análisis de los aspectos sustantivos del código tipo.*

1. Durante los treinta días siguientes a la notificación o subsanación de los defectos el Registro General de Protección de Datos podrá convocar a los solicitantes, a fin de obtener aclaraciones o precisiones relativas al contenido sustantivo del código tipo.

2. Transcurrido el plazo señalado en el apartado anterior, el Registro General de Protección de Datos elaborará un informe sobre las características del proyecto de código tipo.

3. La documentación presentada y el informe del Registro serán remitidos al Gabinete Jurídico, a fin de que por el mismo se informe acerca del cumplimiento de los requisitos establecidos en el Título VII de este Reglamento.

Artículo 147. *Información pública.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

Artículo 148. *Mejora del código tipo.*

Si durante la tramitación del procedimiento resultase necesaria la aportación de nuevos documentos o la modificación del código tipo presentado, la Agencia Española de Protección de Datos podrá requerir al solicitante, a fin de que en el plazo de treinta días introduzca las modificaciones que sean precisas, remitiendo el texto resultante a la Agencia Española de Protección de Datos.

Se declarará la suspensión del procedimiento en tanto el solicitante no dé cumplimiento al requerimiento.

Artículo 149. *Trámite de audiencia.*

En caso de que durante el trámite previsto en el ar-tículo 148 se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 150. *Resolución.*

1. Cumplidos los términos establecidos en los artículos precedentes, el Director de la Agencia resolverá sobre la procedencia o improcedencia de la inscripción del código tipo en el Registro General de Protección de Datos.

2. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la inscripción del código tipo, se dará traslado de la resolución al Registro General de Protección de Datos, a fin de proceder a su inscripción.

Artículo 151. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de seis meses, a contar desde la fecha de entrada de la solicitud en la Agencia Española de Protección de Datos.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el solicitante podrá considerar estimada su solicitud.

Artículo 152. *Publicación de los códigos tipo por la Agencia Española de Protección de Datos.*

La Agencia Española de Protección de Datos dará publicidad al contenido de los códigos tipo inscritos en el Registro General de Protección de Datos, utilizando para ello, con carácter preferente, medios electrónicos o telemáticos.

CAPÍTULO VII

Otros procedimientos tramitados por la agencia española de protección de datos

Sección 1.ª Procedimiento de exención del deber de información al interesado

Artículo 153. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la exención del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal cuando resulte imposible o exija esfuerzos desproporcionados, prevista en el apartado 5 del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, se iniciará siempre a petición del responsable que pretenda obtener la aplicación de la exención.

2. En el escrito de solicitud, además de los requisitos recogidos en el art. 70 de la Ley 30/1992, de 26 de noviembre, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la exención del deber de informar.

b) Motivar expresamente las causas en que fundamenta la imposibilidad o el carácter desproporcionado del esfuerzo que implicaría el cumplimiento del deber de informar.

c) Exponer detalladamente las medidas compensatorias que propone realizar en caso de exoneración del cumplimiento del deber de informar.

d) Aportar una cláusula informativa que, mediante su difusión, en los términos que se indiquen en la solicitud, permita compensar la exención del deber de informar.

Artículo 154. *Propuesta de nuevas medidas compensatorias.*

1. Si la Agencia Española de Protección de Datos considerase insuficientes las medidas compensatorias propuestas por el solicitante, podrá acordar la adopción de medidas complementarias o sustitutivas a las propuestas por aquél en su solicitud.

2. Del acuerdo se dará traslado al solicitante, a fin de que exponga lo que a su derecho convenga en el plazo de quince días.

Artículo 155. *Terminación del procedimiento.*

Concluidos los trámites previstos en los artículos precedentes, el Director de la Agencia dictará resolución, concediendo o denegando la exención del deber de informar. La resolución podrá imponer la adopción de las medidas complementarias a las que se refiere el artículo anterior.

Artículo 156. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud por silencio administrativo positivo.

Sección 2.ª Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos

Artículo 157. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la declaración de la concurrencia en un determinado tratamiento de datos de valores históricos, científicos o estadísticos, a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento, se iniciará siempre a petición del responsable que pretenda obtener la declaración.

2. En el escrito de solicitud, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la excepción.

b) Motivar expresamente las causas que justificarían la declaración.

c) Exponer detalladamente las medidas que el responsable del fichero se propone implantar para garantizar el derecho de los ciudadanos.

3. La solicitud deberá acompañarse de cuantos documentos o pruebas sean necesarios para justificar la existencia de los valores históricos, científicos o estadísticos que fundamentarían la declaración de la Agencia.

Artículo 158. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud.

Disposición adicional única. *Productos de software.*

Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento.

Disposición final única. *Aplicación supletoria.*

En lo no establecido en el capítulo III del título IX serán de aplicación a los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos las disposiciones contenidas en el Reglamento del Procedimiento para el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, de 4 de agosto.

§ 6

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

Jefatura del Estado
«BOE» núm. 251, de 19 de octubre de 2007
Última modificación: 10 de mayo de 2014
Referencia: BOE-A-2007-18243

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

I

La aplicación de las nuevas tecnologías desarrolladas en el marco de la sociedad de la información ha supuesto la superación de las formas tradicionales de comunicación, mediante una expansión de los contenidos transmitidos, que abarcan no sólo la voz, sino también datos en soportes y formatos diversos. A su vez, esta extraordinaria expansión en cantidad y calidad ha venido acompañada de un descenso en los costes, haciendo que este tipo de comunicaciones se encuentre al alcance de cualquier persona y en cualquier rincón del mundo.

La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley.

El objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados. Se entienden por agentes facultados los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de

Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos éstos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones.

En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

En relación con esta última precisión, cabe señalar que la Directiva se refiere, expresamente, a que los datos conservados deberán estar disponibles a los fines de detección o investigación por delitos graves, definidos éstos de acuerdo con la legislación interna de cada Estado miembro.

II

La Ley cuenta con diez artículos que se agrupan en tres capítulos.

El Capítulo I («Disposiciones Generales») se inicia describiendo su objeto, que básicamente se circunscribe a la determinación de la obligación de conservar los datos enumerados en el artículo 3, que se hayan generado o tratado en el marco de una comunicación de telefonía fija o móvil, o realizada a través de una comunicación electrónica de acceso público o mediante una red pública de comunicaciones. Igualmente, se precisan los fines que, exclusivamente, justifican la obligación de conservación, y que se limitan a la detección, investigación y enjuiciamiento de un delito contemplado en el Código Penal o las leyes penales especiales, con los requisitos y cautelas que la propia Ley establece.

En este capítulo también se precisan las limitaciones sobre el tipo de datos a retener, que son los necesarios para identificar el origen y destino de la comunicación, así como la identidad de los usuarios o abonados de ambos, pero nunca datos que revelen el contenido de la comunicación. Igualmente, la Ley impone la obligación de conservación de datos que permitan determinar el momento y duración de una determinada comunicación, su tipo, así como datos necesarios para identificar el equipo de comunicación empleado y, en el caso de utilización de un equipo móvil, los datos necesarios para su localización.

En relación con los sujetos que quedan obligados a conservar los datos, éstos serán los operadores que presten servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en España.

La Ley enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet. Estos datos, que, se repite, en ningún caso revelarán el contenido de la comunicación, son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado. En aplicación de las previsiones contenidas en la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, quedan incluidas también en el ámbito de aplicación de la Ley las denominadas llamadas telefónicas infructuosas. Igualmente se incluye la obligación de conservar los elementos que sean suficientes para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago.

En el Capítulo II («Conservación y cesión de datos») se establecen los límites para efectuar la cesión de datos, el plazo de conservación de los mismos, que será, con carácter

general, de doce meses desde que la comunicación se hubiera establecido (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE), y los instrumentos para garantizar el uso legítimo de los datos conservados, cuya cesión y entrega exclusivamente se podrá efectuar al agente facultado y para los fines establecidos en la Ley, estando cualquier uso indebido sometido a los mecanismos de control de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. Además, se establecen previsiones específicas respecto al régimen general regulador de los derechos de acceso, rectificación y cancelación de datos contenido en la referida Ley Orgánica 15/1999.

El Capítulo III, al referirse al régimen sancionador, remite, en cuanto a los incumplimientos de las obligaciones de conservación y protección y seguridad de los datos de carácter personal, a la regulación contenida en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Por otro lado, los incumplimientos de la obligación de puesta a disposición de los agentes facultados, en la medida en que las solicitudes estarán siempre amparadas por orden judicial, constituirían la correspondiente infracción penal.

En las disposiciones contenidas en la parte final se incluyen contenidos diversos. Por un lado, y a los efectos de poder establecer instrumentos para controlar el empleo para fines delictivos de los equipos de telefonía móvil adquiridos mediante la modalidad de prepago, se establece, como obligación de los operadores que comercialicen dicho servicio, la llevanza de un registro con la identidad de los compradores.

Por último, la Ley incorpora en las disposiciones finales una modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, para adaptarla al contenido de esta Ley, una referencia a su amparo competencial, una habilitación general al Gobierno para su desarrollo y un período de seis meses para que las operadoras puedan adaptarse a su contenido.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la Ley.*

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2. *Sujetos obligados.*

Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 3. *Datos objeto de conservación.*

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil:

i) Número de teléfono de llamada.
ii) Nombre y dirección del abonado o usuario registrado.

2.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignada.
ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.
iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.
ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.
ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.
2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.
ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).
2.° Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.
2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.
ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.
iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.
iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

CAPÍTULO II

Conservación y cesión de datos

Artículo 4. *Obligación de conservar datos.*

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.

En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

Artículo 5. *Período de conservación de los datos.*

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación.

Artículo 6. *Normas generales sobre cesión de datos.*

1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial.

2. La cesión de la información se efectuará mediante formato electrónico únicamente a los agentes facultados, y deberá limitarse a la información que resulte imprescindible para la consecución de los fines señalados en el artículo 1.

A estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Artículo 7. *Procedimiento de cesión de datos.*

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro del plazo de 7 días naturales contados a partir de las 8:00 horas del día natural siguiente a aquél en que el sujeto obligado reciba la orden.

Artículo 8. *Protección y seguridad de los datos.*

1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley.

Artículo 9. *Excepciones a los derechos de acceso y cancelación.*

1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley.

2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Infracciones y sanciones

Artículo 10. *Infracciones y sanciones.*

1. Constituyen infracciones a lo previsto en la presente Ley las siguientes:

a) Es infracción muy grave la no conservación en ningún momento de los datos a los que se refiere el artículo 3.

b) Son infracciones graves:

i) La no conservación reiterada o sistemática de los datos a los que se refiere el artículo 3.

ii) La conservación de los datos por un período inferior al establecido en el artículo 5.

iii) El incumplimiento deliberado de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8.

c) Son infracciones leves:

i) La no conservación de los datos a los que se refiere el artículo 3 cuando no se califique como infracción muy grave o grave.

ii) El incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8, cuando no se califique como infracción grave.

2. A las infracciones previstas en el apartado anterior, a excepción de las indicadas en los apartados 1.b).iii y 1.c).ii de este artículo, les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

3. A las infracciones previstas en los apartados 1.b).iii y 1.c).ii de este artículo les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora a la Agencia Española de Protección de Datos.

Disposición adicional única. *Servicios de telefonía mediante tarjetas de prepago.*

1. Los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago, deberán llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.

Los operadores informarán a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, de su disponibilidad en los términos expresados en el número siguiente y de los derechos recogidos en el artículo 38.6 de la Ley 32/2003.

La identificación se efectuará mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal.

2. Desde la activación de la tarjeta de prepago y hasta que cese la obligación de conservación a que se refiere el artículo 5 de esta Ley, los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la

seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.

3. Los datos identificativos estarán sometidos a las disposiciones de esta Ley, respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada.

4. Los operadores deberán ceder los datos identificativos previstos en el apartado 1 de esta disposición a los agentes facultados, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

5. Constituyen infracciones a lo previsto en la presente disposición, además de la previstas en el artículo 10, las siguientes:

a) Es infracción muy grave el incumplimiento de la llevanza del libro-registro referido.

b) Son infracciones graves la llevanza reiterada o sistemáticamente incompleta de dicho libro-registro así como el incumplimiento deliberado de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición.

c) Son infracciones leves la llevanza incompleta del libro-registro o el incumplimiento de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición cuando no se califiquen como infracciones muy graves o graves.

6. A las infracciones previstas en el apartado anterior les será de aplicación el régimen sancionador establecido en la Ley 32/2003, de 3 de noviembre, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

7. La obligación de inscripción en el libro-registro de los datos identificativos de los compradores que adquieran tarjetas inteligentes, así como el resto de obligaciones contenidas en la presente disposición adicional, comenzarán a ser exigibles a partir de la entrada en vigor de esta Ley.

8. No obstante, por lo que se refiere a las tarjetas adquiridas con anterioridad a la entrada en vigor de esta Ley, los operadores de telefonía móvil que comercialicen estos servicios dispondrán de un plazo de dos años, a contar desde dicha entrada en vigor, para cumplir con las obligaciones de inscripción a que se refiere el apartado 1 de la presente disposición adicional.

Transcurrido el aludido plazo de dos años, los operadores vendrán obligados a anular o a desactivar aquellas tarjetas de prepago respecto de las que no se haya podido cumplir con las obligaciones de inscripción del referido apartado 1 de esta disposición adicional, sin perjuicio de la compensación que, en su caso, corresponda al titular de las mismas por el saldo pendiente de consumo.

Disposición transitoria única. *Vigencia del régimen de interceptación de telecomunicaciones.*

Las normas dictadas en desarrollo del Capítulo III del Título III de la Ley 32/2003, de 3 de noviembre, continuarán en vigor en tanto no se opongan a lo dispuesto en esta Ley.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogados los artículos 12, 38.2 c) y d) y 38.3 a) de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley.

Disposición final primera. *Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica en los siguientes términos:

Uno. El artículo 33 queda redactado de la siguiente forma:

«Artículo 33. *Secreto de las comunicaciones.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.
h) Marcas temporales.
i) Información de localización.
j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.
b) Domicilio en el que el proveedor realiza las notificaciones.
Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:
c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).
d) Número de identificación del terminal.
e) Número de cuenta asignada por el proveedor de servicios Internet.
f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.
8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.
9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.
10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.
Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.»

Dos. El último párrafo del apartado 5 del artículo 38 pasa a tener la siguiente redacción:

«Lo establecido en las letras a) y d) del apartado 3 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

Tres. En el artículo 53, se modifican los párrafos o) y z), que quedan redactados de la siguiente forma:

«o) El incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de esta Ley y el incumplimiento deliberado de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

«z) La vulneración grave o reiterada de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y el incumplimiento grave o reiterado de las obligaciones de protección y seguridad de los datos almacenados establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.»

Cuatro. En el artículo 54 se modifican los párrafos ñ) y r), que quedan redactados de la siguiente forma:

«ñ) El incumplimiento, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de la presente Ley y el incumplimiento de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, salvo que deban considerarse como infracción muy grave, conforme a lo dispuesto en el artículo anterior.»

«r) La vulneración de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, y el incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, salvo que deban considerarse como infracción muy grave.»

Disposición final segunda. *Competencia estatal.*

Esta Ley se dicta al amparo de lo dispuesto en el artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, y del artículo 149.1.21.ª, que confiere al Estado competencia exclusiva en materia de telecomunicaciones.

Disposición final tercera. *Desarrollo reglamentario.*

Se habilita al Gobierno a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en esta Ley.

Disposición final cuarta. *Formato de entrega de los datos.*

1. La cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los Ministros de Interior, de Defensa y de Economía y Hacienda, que se aprobará en el plazo de tres meses desde la entrada en vigor de esta Ley.

2. Los sujetos obligados a los que se refiere el artículo 2 de esta Ley, tendrán un plazo de seis meses desde la entrada en vigor de la misma para configurar, a su costa, sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos.

Disposición final quinta. *Entrada en vigor.*

Esta Ley entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

§ 7

Resolución de 22 de junio de 2001, de la Subsecretaría, por la que se dispone la publicación del Acuerdo de Consejo de Ministros por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información

Ministerio de Justicia
«BOE» núm. 151, de 25 de junio de 2001
Última modificación: sin modificaciones
Referencia: BOE-A-2001-12222

El Consejo de Ministros, en su reunión de 22 de junio de 2001, ha aprobado el Acuerdo por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información.

Con el fin de favorecer su conocimiento y aplicación generales, se ordena su publicación como anexo a la presente Resolución.

ANEXO

Acuerdo por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información

El Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, establece en su disposición transitoria única los plazos de implantación de las medidas de seguridad para los sistemas de información que se encontraban en funcionamiento a la entrada en vigor de dicho Reglamento, que se produjo el 26 de junio de 1999.

Dicha disposición transitoria única contempla un plazo de dos años para que se proceda a la implantación de las medidas de seguridad de nivel alto en los indicados sistemas de información, si bien la propia norma prevé la ampliación en un año del plazo inicial, cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad a las que se refiere el Reglamento.

El 26 de junio de 2001 se cumplen dos años desde la entrada en vigor del Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y resulta constatable que respecto de numerosos sistemas de información, tanto de titularidad pública como privada, que ya se encontraban en funcionamiento en aquella fecha y en los cuales, de acuerdo con lo previsto en el artículo 4.3 del Reglamento, deben implantarse las medidas de seguridad calificadas como de nivel alto que se determinan en su capítulo IV, se han encontrado dificultades de orden tecnológico que han imposibilitado la plena implantación de tales medidas hasta el momento.

§ 7 Plazo de implantación de medidas de seguridad de nivel alto en sistemas de información

En virtud de ello parece oportuno, apreciando que concurren las circunstancias previstas para la aplicación del párrafo segundo de la disposición transitoria única del Reglamento, hacer uso de la facultad de ampliar el plazo para la implantación de las medidas de seguridad de nivel alto en los sistemas de información que estuvieran en funcionamiento antes de la entrada en vigor de aquél, que será, en consecuencia, de tres años a contar de dicha fecha.

Por todo lo cual, a propuesta del Ministro de Justicia, previo informe de la Agencia de Protección de Datos, el Consejo de Ministros, en su reunión del día 22 de junio de 2001, acuerda:

El plazo para la implantación de las medidas de seguridad de nivel alto en aquellos sistemas de información que se hallaban en funcionamiento con anterioridad a la fecha de entrada en vigor del Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, será de tres años desde la citada fecha de entrada en vigor, concluyendo, en consecuencia, el 26 de junio de 2002.

§ 8

Orden de 2 de febrero de 1995 por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos

Ministerio de Justicia e Interior
«BOE» núm. 35, de 10 de febrero de 1995
Última modificación: 21 de agosto de 1998
Referencia: BOE-A-1995-3543

La transferencia internacional de datos se regula en los artículos 32 y 33 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, y se completa en los artículos 3 y 4 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de dicha Ley, cuya disposición final primera faculta al Ministro de Justicia e Interior para aprobar la relación de países que, a efectos de lo dispuesto en el artículo 32 de la propia Ley Orgánica, se entiende que proporcionan un nivel de protección equiparable al de dicha Ley.

Las legislaciones de los distintos países son heterogéneas y difícilmente comparables, por lo cual la relación que se aprueba por la presente Orden deben integrarse por varias relaciones parciales, especificando de forma separada los países que proporcionan un nivel de protección equiparable al español, según se trate de ficheros de titularidad pública o de ficheros de titularidad privada.

Por otra parte, tanto las legislaciones de los distintos países como los estudios que se llevan a cabo en España sobre su naturaleza y alcance, se encuentran en un proceso de evolución permanente, por cuya razón lo que se aprueba a través de la presente Orden es una primera relación de países, es decir una relación de carácter abierto, que deberá ser continuada y completada, en paralelo con la evolución de las legislaciones extranjeras y de los estudios correspondientes.

En su virtud, y de conformidad con el preceptivo informe emitido por el Director de la Agencia de Protección de Datos, dispongo:

Primero.

Los países cuyo régimen legal de protección de datos de carácter personal, objeto de tratamiento automatizado, se considera que proporciona un nivel de protección equiparable al de la Ley Orgánica 5/1992, de 29 de octubre, tanto respecto a ficheros de titularidad pública como a los de titularidad privada, son los países parte del Convenio para la Protección de las Personas con relación al Tratamiento Automatizado de los Datos de Carácter Personal, abierto a la firma en Estrasburgo el 28 de enero de 1981, y concretamente los siguientes:

Alemania, Austria, Bélgica, Dinamarca —con la excepción del territorio de las Islas Féroe y de Groenlandia—, Eslovenia, Finlandia, Francia, Grecia, Irlanda, Italia, Islandia, Luxemburgo, Noruega —con la excepción del territorio de Svalbard—, Países Bajos, Portugal, Reino Unido —inclusive el territorio de las Islas de Man y Jersey— y Suecia.

Segundo.

Asimismo se considera que proporcionan un nivel de protección equiparable al de la Ley Orgánica 5/1992, de 29 de octubre, respecto a ficheros de titularidad pública y de titularidad privada, Australia, Israel, Hungría, Nueva Zelanda, República Checa, República de Slovakia, San Marino y Suiza.

Tercero.

Se considera que proporcionan un nivel de protección equiparable al de la Ley Orgánica 5/1992, de 29 de octubre, respecto de los datos registrados en ficheros de titularidad pública, la República de Andorra y Japón.

Cuarto.

También se considera que proporciona un nivel de protección equiparable al de la Ley Orgánica 5/1992, de 29 de octubre, la legislación de Canadá respecto de los ficheros de titularidad pública, y que disponen de un régimen de protección equiparable al de dicha Ley, respecto de los ficheros de titularidad privada, las provincias canadienses de Quebec, Ontario, Saskatchewan y Columbia Británica.

Quinto.

De conformidad con lo dispuesto en los artículos 32 y 33 de la Ley Orgánica 5/1992, de 29 de octubre, y 3 y 4 del Real Decreto 1332/1994, de 20 de junio, lo dispuesto en la presente Orden se entiende sin perjuicio de lo establecido en tratados o convenios en los que sea parte España, y de las restantes excepciones legales, así como de las facultades que corresponden a la Agencia de Protección de Datos para autorizar las transferencias internacionales de datos, si se obtienen garantías adecuadas.

Disposición final.

La presente Orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 9

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Unión Europea
«DOUE» núm. 119, de 4 de mayo de 2016
Última modificación: sin modificaciones
Referencia: DOUE-L-2016-89807

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 16,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de texto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo [1],

Visto el dictamen del Comité de las Regiones [2],

De conformidad con el procedimiento legislativo ordinario [3],

Considerando lo siguiente:

(1) La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas.

(3) La Directiva 95/46/CE del Parlamento Europeo y del Consejo [4] trata de armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros.

(4) El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe

considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.

(5) La integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos de datos personales. En toda la Unión se ha incrementado el intercambio de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas. El Derecho de la Unión insta a las autoridades nacionales de los Estados miembros a que cooperen e intercambien datos personales a fin de poder cumplir sus funciones o desempeñar otras por cuenta de una autoridad de otro Estado miembro.

(6) La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

(7) Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

(8) En los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento.

(9) Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular en relación con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección de los datos de carácter personal, en lo que respecta al tratamiento de dichos datos en los Estados miembros pueden impedir la libre circulación de los datos de carácter personal en la Unión. Estas diferencias pueden constituir, por lo tanto, un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión. Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE.

(10) Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión

realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento. Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito.

(11) La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes.

(12) El artículo 16, apartado 2, del TFUE encomienda al Parlamento Europeo y al Consejo que establezcan las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal y las normas relativas a la libre circulación de dichos datos.

(13) Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Con objeto de tener en cuenta la situación específica de las microempresas y las pequeñas y medianas empresas, el presente Reglamento incluye una serie de excepciones en materia de llevanza de registros para organizaciones con menos de 250 empleados. Además, alienta a las instituciones y órganos de la Unión y a los Estados miembros y a sus autoridades de control a tener en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas en la aplicación del presente Reglamento. El concepto de microempresas y pequeñas y medianas empresas debe extraerse del artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión [5].

(14) La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

(15) A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento.

(16) El presente Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con

actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

(17) El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo [6] se aplica al tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal deben adaptarse a los principios y normas establecidos en el presente Reglamento y aplicarse a la luz del mismo. A fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión, una vez adoptado el presente Reglamento deben introducirse las adaptaciones necesarias del Reglamento (CE) n.º 45/2001, con el fin de que pueda aplicarse al mismo tiempo que el presente Reglamento.

(18) El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

(19) La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El presente Reglamento no debe, por lo tanto, aplicarse a las actividades de tratamiento destinadas a tales fines. No obstante, los datos personales tratados por las autoridades públicas en aplicación del presente Reglamento deben, si se destinan a tales fines, regirse por un acto jurídico de la Unión más específico, concretamente la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo [7]. Los Estados miembros pueden encomendar a las autoridades competentes, tal como se definen en la Directiva (UE) 2016/680, funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del presente Reglamento.

En lo que respecta al tratamiento de datos personales por parte de dichas autoridades competentes con fines que entren en el ámbito de aplicación del presente Reglamento, los Estados miembros deben tener la posibilidad de mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del presente Reglamento. Tales disposiciones pueden establecer de forma más precisa requisitos concretos para el tratamiento de datos personales con otros fines por parte de dichas autoridades competentes, tomando en consideración la estructura constitucional, organizativa y administrativa del Estado miembro en cuestión. Cuando el tratamiento de datos personales por organismos privados entre en el ámbito de aplicación del presente Reglamento, este debe disponer que los Estados miembros puedan, en condiciones específicas, limitar conforme a Derecho determinadas obligaciones y derechos siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención. Esto se aplica, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o de las actividades de los laboratorios de policía científica.

(20) Aunque el presente Reglamento se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales, en virtud del Derecho de la Unión o de los Estados

miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento en relación con el tratamiento de datos personales por los tribunales y otras autoridades judiciales. A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos.

(21) El presente Reglamento debe entenderse sin perjuicio de la aplicación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo [8], en particular de las normas en materia de responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15. El objetivo de dicha Directiva es contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros.

(22) Todo tratamiento de datos personales en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de que el tratamiento tenga lugar en la Unión. Un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto.

(23) Con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento, el tratamiento de datos personales de interesados que se encuentran en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que se encuentran en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

(24) El tratamiento de datos personales de los interesados que se encuentran en la Unión por un responsable o encargado no establecido en la Unión debe ser también objeto del presente Reglamento cuando esté relacionado con la observación del comportamiento de dichos interesados en la medida en que este comportamiento tenga lugar en la Unión. Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

(25) Cuando sea de aplicación el Derecho de los Estados miembros en virtud del Derecho internacional público, el presente Reglamento debe aplicarse también a todo responsable del tratamiento no establecido en la Unión, como en una misión diplomática u oficina consular de un Estado miembro.

(26) Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de

información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

(27) El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas.

(28) La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.

(29) Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas.

(30) Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.

(31) Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento.

(32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las

actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

(33) Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.

(34) Debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

(35) Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo [9]; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

(36) El establecimiento principal de un responsable del tratamiento en la Unión debe ser el lugar de su administración central en la Unión, salvo que las decisiones relativas a los fines y medios del tratamiento de los datos personales se tomen en otro establecimiento del responsable en la Unión, en cuyo caso, ese otro establecimiento debe considerarse el establecimiento principal. El establecimiento principal de un responsable en la Unión debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables. Dicho criterio no debe depender de si el tratamiento de los datos personales se realiza en dicho lugar. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituyen, en sí mismas, establecimiento principal y no son, por lo tanto, criterios determinantes de un establecimiento principal. El establecimiento principal del encargado del tratamiento debe ser el lugar de su administración central en la Unión o, si careciese de administración central en la Unión, el lugar en el que se llevan a cabo las principales actividades de tratamiento en la Unión. En los casos que impliquen tanto al responsable como al encargado, la autoridad de control principal competente debe seguir siendo la autoridad de control del Estado miembro en el que el responsable tenga su establecimiento principal, pero la autoridad de control del encargado debe considerarse autoridad de control interesada y participar en el procedimiento de cooperación establecido en el presente Reglamento. En cualquier caso, las autoridades de control del Estado miembro o los Estados miembros en los que el encargado tenga uno o varios establecimientos no deben considerarse autoridades de control interesadas cuando el proyecto de decisión afecte únicamente al responsable. Cuando el tratamiento lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine otra empresa.

(37) Un grupo empresarial debe estar constituido por una empresa que ejerce el control y las empresas controladas, debiendo ser la empresa que ejerce el control la que pueda ejercer una influencia dominante en las otras empresas, por razones, por ejemplo, de propiedad, participación financiera, normas por las que se rige, o poder de hacer cumplir las normas de protección de datos personales. Una empresa que controle el tratamiento de los datos personales en las empresas que estén afiliadas debe considerarse, junto con dichas empresas, «grupo empresarial».

(38) Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.

(39) Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

(40) Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.

(41) Cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate. Sin embargo, dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia») y del Tribunal Europeo de Derechos Humanos.

(42) Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración

por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo [10], debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

(43) Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento.

(44) El tratamiento debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato.

(45) Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional.

(46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

(47) El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo,

cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.

(48) Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. Los principios generales aplicables a la transmisión de datos personales, dentro de un grupo empresarial, a una empresa situada en un país tercero no se ven afectados.

(49) Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

(50) El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable. Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto.

(51) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

(52) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

(53) Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para

lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional. El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos.

(54) El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo [(11)], es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.

(55) Se realiza además por razones de interés público el tratamiento de datos personales por las autoridades públicas con el fin de alcanzar los objetivos, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente.

(56) Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas.

(57) Si los datos personales tratados por un responsable no le permiten identificar a una persona física, el responsable no debe estar obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir cualquier disposición del presente Reglamento. No obstante, el responsable del tratamiento no debe negarse a recibir información adicional facilitada por el interesado a fin de respaldarle en el ejercicio de sus derechos. La identificación debe incluir la identificación digital de un interesado, por ejemplo mediante un mecanismo de autenticación, como las mismas credenciales, empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el responsable.

(58) El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le

conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

(59) Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas.

(60) Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente.

(61) Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general.

(62) Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas.

(63) Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento. Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener

como resultado la negativa a prestar toda la información al interesado. Si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud.

(64) El responsable del tratamiento debe utilizar todas las medidas razonables para verificar la identidad de los interesados que soliciten acceso, en particular en el contexto de los servicios en línea y los identificadores en línea. El responsable no debe conservar datos personales con el único propósito de poder responder a posibles solicitudes.

(65) Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

(66) A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

(67) Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

(68) Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato. Por su propia naturaleza, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al

responsable. El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles. Cuando un conjunto de datos personales determinado concierna a más de un interesado, el derecho a recibir tales datos se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento. Por otra parte, ese derecho no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el presente Reglamento, y en particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato. El interesado debe tener derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible.

(69) En los casos en que los datos personales puedan ser tratados lícitamente porque el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o por motivos de intereses legítimos del responsable o de un tercero, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado.

(70) Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información.

(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento automatizado de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor.

A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para

los intereses y derechos del interesado e impedir, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o tratamiento que dé lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas.

(72) La elaboración de perfiles está sujeta a las normas del presente Reglamento que rigen el tratamiento de datos personales, como los fundamentos jurídicos del tratamiento o los principios de la protección de datos. El Comité Europeo de Protección de Datos establecido por el presente Reglamento (en lo sucesivo, el «Comité») debe tener la posibilidad de formular orientaciones en este contexto.

(73) El Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfiles, así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios. Dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

(74) Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

(76) La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

(77) Se podrían proporcionar directrices para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento, especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo, que revistan, en particular, la forma de códigos de conducta aprobados, certificaciones aprobadas, directrices dadas por el Comité o indicaciones proporcionadas por un delegado de protección de datos. El Comité también puede emitir directrices sobre operaciones de tratamiento que se considere improbable supongan un alto riesgo para los derechos y libertades de las personas físicas, e indicar qué medidas pueden ser suficientes en dichos casos para afrontar el riesgo en cuestión.

(78) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

(79) La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.

(80) El responsable o el encargado del tratamiento no establecido en la Unión que esté tratando datos personales de interesados que se encuentran en la Unión y cuyas actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere un pago por parte de estos, o con el control de su comportamiento en la medida en que este tenga lugar en la Unión, debe designar a un representante, a menos que el tratamiento sea ocasional, no incluya el tratamiento a gran escala de categorías especiales de datos personales o el tratamiento de datos personales relativos a condenas e infracciones penales, y sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, vista la naturaleza, el contexto, el ámbito y los fines del tratamiento, o si el responsable del tratamiento es una autoridad u organismo público. El representante debe actuar por cuenta del responsable o el encargado y puede ser contactado por cualquier autoridad de control. El representante debe ser designado expresamente por mandato escrito del responsable o del encargado para que actúe en su nombre con respecto a las obligaciones que les incumben en virtud del presente Reglamento. La designación de dicho representante no afecta a la responsabilidad del responsable o del encargado en virtud del presente Reglamento. Dicho representante debe

desempeñar sus funciones conforme al mandato recibido del responsable o del encargado, incluida la cooperación con las autoridades de control competentes en relación con cualquier medida que se tome para garantizar el cumplimiento del presente Reglamento. El representante designado debe estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado.

(81) Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos.

(82) Para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad. Todos los responsables y encargados están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento.

(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

(84) A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de

sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

(87) Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento.

(88) Al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, hay que tener debidamente en cuenta las circunstancias de tal violación, inclusive si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido. Asimismo, estas normas y procedimientos deben tener en cuenta los intereses legítimos de las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales.

(89) La Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control. Pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales. Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.

(90) En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular

gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento.

(91) Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hace más difícil para los interesados el ejercicio de sus derechos. La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas. También es necesaria una evaluación de impacto relativa a la protección de datos para el control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos o para cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados, en particular porque impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato, o porque se efectúe sistemáticamente a gran escala. El tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud o abogado. En estos casos, la evaluación de impacto de la protección de datos no debe ser obligatoria.

(92) Hay circunstancias en las que puede ser razonable y económico que una evaluación de impacto relativa a la protección de datos abarque más de un único proyecto, por ejemplo, en el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyecten introducir una aplicación o un entorno de tratamiento común en un sector o segmento empresarial o para una actividad horizontal de uso generalizado.

(93) Los Estados miembros, al adoptar el Derecho en el que se basa el desempeño de las funciones de la autoridad pública o el organismo público y que regula la operación o el conjunto de operaciones de tratamiento en cuestión, pueden considerar necesario llevar a cabo dicha evaluación con carácter previo a las actividades de tratamiento.

(94) Debe consultarse a la autoridad de control antes de iniciar las actividades de tratamiento si una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación. Existe la probabilidad de que ese alto riesgo se deba a determinados tipos de tratamiento y al alcance y frecuencia de este, lo que también puede ocasionar daños y perjuicios o una injerencia en los derechos y libertades de la persona física. La autoridad de control debe responder a la solicitud de consulta dentro de un plazo determinado. Sin embargo, la ausencia de respuesta de la autoridad de control dentro de dicho plazo no debe obstar a cualquier intervención de dicha autoridad basada en las funciones y poderes que le atribuye el presente Reglamento, incluido el poder de prohibir operaciones de tratamiento. Como parte de dicho proceso de consulta, se puede presentar a la autoridad de control el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas.

(95) El encargado del tratamiento debe asistir al responsable cuando sea necesario y a petición suya, a fin de asegurar que se cumplen las obligaciones que se derivan de la

realización de las evaluaciones de impacto relativas a la protección de datos y de la consulta previa a la autoridad de control.

(96) Deben llevarse también a cabo consultas con la autoridad de control en el curso de la tramitación de una medida legislativa o reglamentaria que establezca el tratamiento de datos personales, a fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, en particular, de mitigar el riesgo que implique el tratamiento para el interesado.

(97) Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente.

(98) Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento.

(99) Al elaborar un código de conducta, o al modificar o ampliar dicho código, las asociaciones y otros organismos que representan a categorías de responsables o encargados deben consultar a las partes interesadas, incluidos los interesados cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas en respuesta a dichas consultas.

(100) A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes.

(101) Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.

(102) El presente Reglamento se entiende sin perjuicio de los acuerdos internacionales celebrados entre la Unión y terceros países que regulan la transferencia de datos personales, incluidas las oportunas garantías para los interesados. Los Estados miembros pueden celebrar acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al presente Reglamento ni a ninguna otra disposición del Derecho de la Unión e incluyan un nivel adecuado de protección de los derechos fundamentales de los interesados.

(103) La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u organización internacional que se considera ofrece tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización. La Comisión también puede decidir revocar esa decisión, previo aviso y completa declaración motivada al tercer país u organización internacional.

(104) En consonancia con los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos, la Comisión, en su evaluación del tercer país, o de un territorio o un sector específico de un tercer país, debe tener en cuenta de qué manera respeta un determinado tercer país respeta el Estado de Derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos y su Derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal. En la adopción de una decisión de adecuación con respecto a un territorio o un sector específico de un tercer país se deben tener en cuenta criterios claros y objetivos, como las actividades concretas de tratamiento y el alcance de las normas jurídicas aplicables y la legislación vigente en el tercer país. El tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas.

(105) Aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión debe tener en cuenta las obligaciones resultantes de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones. En particular, debe tenerse en cuenta la adhesión del país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo adicional. La Comisión debe consultar al Comité al evaluar el nivel de protección existente en terceros países u organizaciones internacionales.

(106) La Comisión debe supervisar la aplicación de las decisiones sobre el nivel de protección en un país tercero, un territorio o un sector específico de un país tercero, o una organización internacional, y la aplicación las decisiones adoptadas sobre la base del artículo 25, apartado 6, o el artículo 26, apartado 4, de la Directiva 95/46/CE. En sus decisiones de adecuación, la Comisión debe establecer un mecanismo para la revisión periódica de su aplicación. Dicha revisión periódica debe realizarse en colaboración con el tercer país u organización internacional de que se trate y tener en cuenta todos los cambios en la materia que se produzcan en dicho tercer país u organización internacional. A efectos de la supervisión y realización de las revisiones periódicas, la Comisión debe tomar en consideración las opiniones y conclusiones del Parlamento Europeo y del Consejo, así como de otros organismos y fuentes pertinentes. La Comisión debe evaluar, en un plazo razonable, la aplicación de dichas decisiones e informar de cualquier conclusión pertinente al Comité que, en el sentido del Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo [(12)], establece el presente Reglamento, y al Parlamento Europeo y el Consejo.

(107) La Comisión puede reconocer que un tercer país, un territorio o sector específico en un tercer país, o una organización internacional ya no garantiza un nivel de protección de

datos adecuado. En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país u organización internacional, salvo que se cumplan los requisitos del presente Reglamento relativos a las transferencias basadas en garantías adecuadas, incluidas las normas corporativas vinculantes, y a las excepciones aplicadas a situaciones específicas. En ese caso, debe establecerse la celebración de consultas entre la Comisión y esos terceros países u organizaciones internacionales. La Comisión debe informar en tiempo oportuno al tercer país u organización internacional de las razones y entablar consultas a fin de subsanar la situación.

(108) En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto. Las transferencias también pueden realizarlas autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes se debe recabar la autorización de la autoridad de control competente.

(109) La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe obstar a que los responsables o encargados incluyan las cláusulas tipo de protección de datos en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control, ni mermen los derechos o las libertades fundamentales de los interesados. Se debe alentar a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos.

(110) Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal.

(111) Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, de mediar el consentimiento explícito del interesado, si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores. También se debe establecer la posibilidad de realizar transferencias cuando así lo requieran razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros, o cuando la transferencia se haga a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo. En este último caso la transferencia no debe afectar a la totalidad de los datos personales o de las categorías de datos incluidos en el registro y, cuando el registro esté destinado a su consulta por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de dichas personas o, si

estas van a ser las destinatarias, teniendo plenamente en cuenta los intereses y los derechos fundamentales del interesado.

(112) Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento. En ausencia de una decisión de adecuación, el Derecho de la Unión o de los Estados miembros puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional. Los Estados miembros deben notificar esas disposiciones a la Comisión. Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados.

(113) Las transferencias que pueden calificarse de no repetitivas y sólo se refieren a un número limitado de interesados, también han de ser posibles en caso de servir a intereses legítimos imperiosos del responsable del tratamiento, si no prevalecen sobre ellos los intereses o los derechos y libertades del interesado y el responsable ha evaluado todas las circunstancias concurrentes en la transferencia de datos. El responsable debe prestar especial atención a la naturaleza de los datos personales, la finalidad y la duración de la operación o las operaciones de tratamiento propuestas, así como la situación en el país de origen, el tercer país y el país de destino final, y ofrecer, garantías apropiadas para proteger los derechos fundamentales y las libertades de las personas físicas con respecto al tratamiento de sus datos personales. Dichas transferencias sólo deben ser posibles en casos aislados, cuando ninguno de los otros motivos para la transferencia sean aplicables. Las legítimas expectativas de la sociedad en un aumento del conocimiento se deben tener en cuenta para fines de investigación científica o histórica o fines estadísticos. El responsable debe informar de la transferencia a la autoridad de control y al interesado.

(114) En cualquier caso, cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de la protección de datos en un tercer país, el responsable o el encargado del tratamiento deben arbitrar soluciones que garanticen a los interesados derechos exigibles y efectivos con respecto al tratamiento de sus datos en la Unión, una vez transferidos estos, de forma que sigan beneficiándose de derechos fundamentales y garantías.

(115) Algunos países terceros adoptan leyes, reglamentaciones y otros actos jurídicos con los que se pretende regular directamente las actividades de tratamiento de personas físicas y jurídicas bajo jurisdicción de los Estados miembros. Esto puede incluir sentencias de órganos jurisdiccionales o decisiones de autoridades administrativas de terceros países que obliguen a un responsable o un encargado del tratamiento a transferir o comunicar datos personales, y que no se basen en un acuerdo internacional, como un tratado de asistencia judicial mutua, en vigor entre el tercer país requirente y la Unión o un Estado miembro. La aplicación extraterritorial de dichas leyes, reglamentaciones y otros actos jurídicos puede ser contraria al Derecho internacional e impedir la protección de las personas físicas garantizada en la Unión en virtud del presente Reglamento. Las transferencias solo deben autorizarse cuando se cumplan las condiciones del presente Reglamento relativas a las transferencias a terceros países. Tal puede ser el caso, entre otros, cuando la comunicación sea necesaria por una razón importante de interés público reconocida por el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento.

(116) Cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer

los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. Sus esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por poderes preventivos o correctivos insuficientes, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. Por consiguiente, es necesario fomentar una cooperación más estrecha entre las autoridades de control encargadas de la protección de datos para ayudarlas a intercambiar información y a llevar a cabo investigaciones con sus homólogos internacionales. A fin de desarrollar mecanismos de cooperación internacional que faciliten y proporcionen asistencia internacional mutua en la ejecución de legislación en materia de protección de datos personales, la Comisión y las autoridades de control deben intercambiar información y cooperar en actividades relativas al ejercicio de sus competencias con las autoridades competentes de terceros países, sobre la base de la reciprocidad y de conformidad con el presente Reglamento.

(117) El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.

(118) La independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial.

(119) Si un Estado miembro establece varias autoridades de control, debe disponer por ley mecanismos que garanticen la participación efectiva de dichas autoridades de control en el mecanismo de coherencia. Tal Estado miembro debe, en particular, designar a la autoridad de control que actuará como punto de contacto único de cara a la participación efectiva de dichas autoridades en el citado mecanismo, garantizando así una cooperación rápida y fluida con otras autoridades de control, el Comité y la Comisión.

(120) Todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus funciones, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión. Cada autoridad de control debe disponer de un presupuesto anual público propio, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

(121) Las condiciones generales aplicables al miembro o los miembros de la autoridad de control deben establecerse por ley en cada Estado miembro y disponer, en particular, que dichos miembros han de ser nombrados, por un procedimiento transparente, por el Parlamento, el Gobierno o el jefe de Estado del Estado miembro, a propuesta del Gobierno, de un miembro del Gobierno o del Parlamento o una de sus cámaras, o por un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros. A fin de garantizar la independencia de la autoridad de control, sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones y no participar, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada. La autoridad de control debe tener su propio personal, seleccionado por esta o por un organismo independiente establecido por el Derecho de los Estados miembros, que esté subordinado exclusivamente al miembro o los miembros de la autoridad de control.

(122) Cada autoridad de control debe ser competente, en el territorio de su Estado miembro, para ejercer los poderes y desempeñar las funciones que se le confieran de conformidad con el presente Reglamento. Lo anterior debe abarcar, en particular, el tratamiento en el contexto de las actividades de un establecimiento del responsable o del encargado en el territorio de su Estado miembro, el tratamiento de datos personales realizado por autoridades públicas o por organismos privados que actúen en interés público, el tratamiento que afecte a interesados en su territorio, o el tratamiento realizado por un responsable o un encargado que no esté establecido en la Unión cuando sus destinatarios sean interesados residentes en su territorio. Debe incluirse el examen de reclamaciones

presentadas por un interesado, la realización de investigaciones sobre la aplicación del presente Reglamento y el fomento de la sensibilización del público acerca de los riesgos, las normas, las garantías y los derechos en relación con el tratamiento de datos personales.

(123) A fin de proteger a las personas físicas con respecto al tratamiento de sus datos personales y de facilitar la libre circulación de los datos personales en el mercado interior, las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión. A tal efecto, las autoridades de control deben cooperar entre ellas y con la Comisión, sin necesidad de acuerdo alguno entre Estados miembros sobre la prestación de asistencia mutua ni sobre dicha cooperación.

(124) Si el tratamiento de datos personales se realiza en el contexto de las actividades de un establecimiento de un responsable o un encargado en la Unión y el responsable o el encargado está establecido en más de un Estado miembro, o si el tratamiento en el contexto de las actividades de un único establecimiento de un responsable o un encargado en la Unión afecta o es probable que afecte sustancialmente a interesados en más de un Estado miembro, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado debe actuar como autoridad principal. Dicha autoridad debe cooperar con las demás autoridades interesadas, ya sea porque el responsable o el encargado tenga un establecimiento en el territorio de su Estado miembro, porque afecte sustancialmente a interesados que residen en su territorio, o porque se haya presentado una reclamación ante ellas. Asimismo, cuando un interesado que no resida en ese Estado miembro haya presentado una reclamación, la autoridad de control ante la que se haya presentado esta también debe ser autoridad de control interesada. En el marco de sus funciones de formulación de directrices sobre cualquier cuestión relacionada con la aplicación del presente Reglamento, el Comité debe estar facultado para formular directrices, en particular sobre los criterios que han de tenerse en cuenta para determinar si el tratamiento en cuestión afecta sustancialmente a interesados de más de un Estado miembro y sobre lo que constituya una objeción pertinente y motivada.

(125) La autoridad principal debe ser competente para adoptar decisiones vinculantes relativas a las medidas de aplicación de los poderes conferidos con arreglo al presente Reglamento. En su calidad de autoridad principal, la autoridad de control debe implicar estrechamente y coordinar a las autoridades de control interesadas en el proceso de toma de decisiones. En los casos en los que la decisión consista en rechazar total o parcialmente la reclamación del interesado, esa decisión debe ser adoptada por la autoridad de control ante la que se haya presentado la reclamación.

(126) La decisión debe ser acordada conjuntamente por la autoridad de control principal y las autoridades de control interesadas y debe dirigirse al establecimiento principal o único del responsable o del encargado del tratamiento y ser vinculante para ambos. El responsable o el encargado deben tomar las medidas necesarias para garantizar el cumplimiento del presente Reglamento y la aplicación de la decisión notificada por la autoridad de control principal al establecimiento principal del responsable o del encargado en lo que se refiere a las actividades de tratamiento en la Unión.

(127) Cada autoridad de control que no actúa como autoridad principal debe ser competente para tratar asuntos locales en los que, si bien el responsable o el encargado del tratamiento está establecido en más de un Estado miembro, el objeto del tratamiento específico se refiere exclusivamente al tratamiento efectuado en un único Estado miembro y afecta exclusivamente a interesados de ese único Estado miembro, por ejemplo cuando el tratamiento tiene como objeto datos personales de empleados en el contexto específico de empleo de un Estado miembro. En tales casos, la autoridad de control debe informar sin dilación al respecto a la autoridad de control principal. Una vez informada, la autoridad de control principal debe decidir si tratará el asunto de acuerdo con la disposición aplicable a la cooperación entre la autoridad de control principal y otras autoridades de control interesadas («mecanismo de ventanilla única»), o si lo debe tratar localmente la autoridad de control que le haya informado. Al decidir si trata el asunto, la autoridad de control principal debe considerar si existe un establecimiento del responsable o del encargado en el Estado miembro de la autoridad de control que le haya informado, con el fin de garantizar la ejecución efectiva de la decisión respecto del responsable o encargado del tratamiento. Si la

autoridad de control principal decide tratar el asunto, se debe ofrecer a la autoridad de control informante la posibilidad de presentar un proyecto de decisión, que la autoridad de control principal ha de tener en cuenta en la mayor medida posible al preparar su proyecto de decisión al amparo del mecanismo de ventanilla única.

(128) Las normas sobre la autoridad de control principal y el mecanismo de ventanilla única no deben aplicarse cuando el tratamiento sea realizado por autoridades públicas u organismos privados en interés público. En tales casos, la única autoridad de control competente para ejercer los poderes conferidos con arreglo al presente Reglamento debe ser la autoridad de control del Estado miembro en el que estén establecidos la autoridad pública o el organismo privado.

(129) Para garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las competencias de las autoridades encargadas de la persecución de los delitos con arreglo al Derecho de los Estados miembros para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y ejercitar acciones judiciales. Dichos poderes deben incluir también el poder de imponer una limitación temporal o definitiva al tratamiento, incluida su prohibición. Los Estados miembros pueden especificar otras funciones relacionadas con la protección de datos personales con arreglo al presente Reglamento. Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto, respetar el derecho de todas las personas a ser oídas antes de que se adopte cualquier medida que las afecte negativamente y evitar costes superfluos y molestias excesivas para las personas afectadas. Los poderes de investigación en lo que se refiere al acceso a instalaciones deben ejercerse de conformidad con los requisitos específicos del Derecho procesal de los Estados miembros, como el de la autorización judicial previa. Toda medida jurídicamente vinculante de la autoridad de control debe constar por escrito, ser clara e inequívoca, indicar la autoridad de control que dictó la medida y la fecha en que se dictó, llevar la firma del director o de un miembro de la autoridad de control autorizado por este, especificar los motivos de la medida y mencionar el derecho a la tutela judicial efectiva. Esto no debe obstar a que se impongan requisitos adicionales con arreglo al Derecho procesal de los Estados miembros. La adopción de una decisión jurídicamente vinculante implica que puede ser objeto de control judicial en el Estado miembro de la autoridad de control que adoptó la decisión.

(130) Cuando la autoridad de control ante la cual se haya presentado la reclamación no sea la autoridad de control principal, esta última debe cooperar estrechamente con la primera con arreglo a las disposiciones sobre cooperación y coherencia establecidas en el presente Reglamento. En tales casos, la autoridad de control principal, al tomar medidas concebidas para producir efectos jurídicos, incluida la imposición de multas administrativas, debe tener en cuenta en la mayor medida posible la opinión de la autoridad de control ante la cual se haya presentado la reclamación y la cual debe seguir siendo competente para realizar cualquier investigación en el territorio de su propio Estado miembro en enlace con la autoridad de control competente.

(131) En casos en los que otra autoridad de control deba actuar como autoridad de control principal para las actividades de tratamiento del responsable o del encargado pero el objeto concreto de una reclamación o la posible infracción afecta únicamente a las actividades de tratamiento del responsable o del encargado en el Estado miembro en el que se haya presentado la reclamación o detectado la posible infracción y el asunto no afecta sustancialmente ni es probable que afecte sustancialmente a interesados de otros Estados miembros, la autoridad de control que reciba una reclamación o que detecte situaciones que conlleven posibles infracciones del presente Reglamento o reciba de otra manera información sobre estas debe tratar de llegar a un arreglo amistoso con el responsable del tratamiento y, si no prospera, ejercer todos sus poderes. En lo anterior se debe incluir el

tratamiento específico realizado en el territorio del Estado miembro de la autoridad de control o con respecto a interesados en el territorio de dicho Estado miembro; el tratamiento efectuado en el contexto de una oferta de bienes o servicios destinada específicamente a interesados en el territorio del Estado miembro de la autoridad de control; o el tratamiento que deba evaluarse teniendo en cuenta las obligaciones legales pertinentes en virtud del Derecho de los Estados miembros.

(132) Entre las actividades de sensibilización del público por parte de las autoridades de control deben incluirse medidas específicas dirigidas a los responsables y los encargados del tratamiento, incluidas las microempresas y las pequeñas y medianas empresas, así como las personas físicas, en particular en el contexto educativo.

(133) Las autoridades de control se deben ayudar una a otra en el desempeño de sus funciones y prestar asistencia mutua, con el fin de garantizar la aplicación y ejecución coherentes del presente Reglamento en el mercado interior. Una autoridad de control que solicite asistencia mutua puede adoptar una medida provisional si no recibe respuesta a su solicitud de asistencia en el plazo de un mes a partir de su recepción por la otra autoridad de control.

(134) Cada autoridad de control debe participar, cuando proceda, en operaciones conjuntas con otras autoridades de control. La autoridad de control a la que se solicite ayuda debe tener la obligación de responder a la solicitud en un plazo de tiempo determinado.

(135) A fin de garantizar la aplicación coherente del presente Reglamento en toda la Unión, debe establecerse un mecanismo de coherencia para la cooperación entre las autoridades de control. Este mecanismo debe aplicarse en particular cuando una autoridad de control prevea adoptar una medida dirigida a producir efectos jurídicos en lo que se refiere a operaciones de tratamiento que afecten sustancialmente a un número significativo de interesados en varios Estados miembros. También debe aplicarse cuando cualquier autoridad de control interesada o la Comisión soliciten que dicho asunto se trate al amparo del mecanismo de coherencia. Dicho mecanismo debe entenderse sin perjuicio de cualesquiera medidas que la Comisión pueda adoptar en el ejercicio de sus poderes con arreglo a los Tratados.

(136) En aplicación del mecanismo de coherencia, el Comité debe, en un plazo determinado, emitir un dictamen, si así lo decide una mayoría de sus miembros o si así lo solicita cualquier autoridad de control interesada o la Comisión. El Comité también debe estar facultado para adoptar decisiones jurídicamente vinculantes en caso de diferencias entre autoridades de control. A tal efecto debe dictar, en principio por mayoría de dos tercios de sus miembros, decisiones jurídicamente vinculantes en casos claramente especificados en los que exista conflicto de opiniones entre las autoridades de control, en particular en el mecanismo de cooperación entre la autoridad de control principal y las autoridades de control interesadas sobre el fondo del asunto, especialmente en caso de infracción del presente Reglamento.

(137) La necesidad urgente de actuar puede obedecer a la necesidad de proteger los derechos y libertades de los interesados, en particular cuando exista el riesgo de que pueda verse considerablemente obstaculizado el reconocimiento de alguno de sus derechos. Por lo tanto, una autoridad de control debe poder adoptar en su territorio medidas provisionales, debidamente justificadas, con un plazo de validez determinado no superior a tres meses.

(138) La aplicación de tal mecanismo debe ser una condición para la licitud de una medida de una autoridad de control destinada a producir efectos jurídicos, en aquellos casos en los que su aplicación sea obligatoria. En otros casos de relevancia transfronteriza, la autoridad de control principal y las autoridades de control interesadas deben aplicar entre sí el mecanismo de cooperación, y las autoridades de control interesadas pueden prestarse asistencia mutua y realizar entre sí operaciones conjuntas, sobre una base bilateral o multilateral, sin tener que aplicarlo.

(139) A fin de fomentar la aplicación coherente del presente Reglamento, el Comité debe constituirse como organismo independiente de la Unión. Para cumplir sus objetivos, el Comité debe tener personalidad jurídica. Su presidente debe ostentar su representación. El Comité debe sustituir al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por la Directiva 95/46/CE. Debe estar compuesto por el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de

Protección de Datos, o por sus respectivos representantes. La Comisión debe participar en las actividades del Comité sin derecho a voto y se deben reconocer derechos de voto específicos al Supervisor Europeo de Protección de Datos. El Comité debe contribuir a la aplicación coherente del presente Reglamento en toda la Unión, entre otras cosas asesorando a la Comisión, en particular sobre el nivel de protección en terceros países u organizaciones internacionales, y fomentando la cooperación de las autoridades de control en toda la Unión. El Comité debe actuar con independencia en el cumplimiento de sus funciones.

(140) El Comité debe contar con una secretaría, a cargo el Supervisor Europeo de Protección de Datos. El personal del Supervisor Europeo de Protección de Datos que participe en la realización de las funciones conferidas al Comité por el presente Reglamento debe desempeñar sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité y responder ante él.

(141) Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta si considera que se vulneran sus derechos con arreglo al presente Reglamento o en caso de que la autoridad de control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado. La investigación a raíz de una reclamación debe llevarse a cabo, bajo control judicial, si procede en el caso concreto. La autoridad de control debe informar al interesado de la evolución y el resultado de la reclamación en un plazo razonable. Si el asunto requiere una mayor investigación o coordinación con otra autoridad de control, se debe facilitar información intermedia al interesado. Para facilitar la presentación de reclamaciones, cada autoridad de control debe adoptar medidas como el suministro de un formulario de reclamaciones, que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

(142) El interesado que considere vulnerados los derechos reconocidos por el presente Reglamento debe tener derecho a conferir mandato a una entidad, organización o asociación sin ánimo de lucro que esté constituida con arreglo al Derecho de un Estado miembro, tenga objetivos estatutarios que sean de interés público y actúe en el ámbito de la protección de los datos personales, para que presente en su nombre una reclamación ante la autoridad de control, ejerza el derecho a la tutela judicial en nombre de los interesados o, si así lo establece el Derecho del Estado miembro, ejerza el derecho a recibir una indemnización en nombre de estos. Un Estado miembro puede reconocer a tal entidad, organización o asociación el derecho a presentar en él una reclamación con independencia del mandato de un interesado y el derecho a la tutela judicial efectiva, cuando existan motivos para creer que se han vulnerado los derechos de un interesado como consecuencia de un tratamiento de datos personales que sea contrario al presente Reglamento. Esa entidad, organización o asociación no puede estar autorizada a reclamar una indemnización en nombre de un interesado al margen del mandato de este último.

(143) Toda persona física o jurídica tiene derecho a interponer ante el Tribunal de Justicia recurso de anulación de decisiones del Comité, en las condiciones establecidas en el artículo 263 del TFUE. Como destinatarias de dichas decisiones, las autoridades de control interesadas que quieran impugnarlas tienen que interponer recurso en el plazo de dos meses a partir del momento en que les fueron notificadas, de conformidad con el artículo 263 del TFUE. En caso de que las decisiones del Comité afecten directa e individualmente a un responsable, un encargado o al reclamante, estos pueden interponer recurso de anulación de dichas decisiones en el plazo de dos meses a partir de su publicación en el sitio web del Comité, de conformidad con el artículo 263 del TFUE. Sin perjuicio de lo dispuesto en el artículo 263 del TFUE, toda persona física o jurídica debe tener derecho a la tutela judicial efectiva ante el tribunal nacional competente contra las decisiones de una autoridad de control que produzcan efectos jurídicos que le afecten. Tales decisiones se refieren en particular al ejercicio de los poderes de investigación, corrección y autorización por parte de la autoridad de control o a la desestimación o rechazo de reclamaciones. No obstante, el derecho a la tutela judicial efectiva no incluye medidas adoptadas por las autoridades de control que no sean jurídicamente vinculantes, como los dictámenes publicados o el

asesoramiento facilitado por ellas. Las acciones contra una autoridad de control deben ejercitarse ante los tribunales del Estado miembro en el que esté establecida y tramitarse con arreglo al Derecho procesal de dicho Estado miembro. Dichos tribunales deben tener plena jurisdicción, incluida la competencia para examinar todos los elementos de hecho y de Derecho relativos a la causa de la que conozcan.

Si una autoridad de control rechaza o desestima una reclamación, el reclamante puede ejercitar una acción ante los tribunales del mismo Estado miembro. En el contexto de las acciones judiciales relacionadas con la aplicación del presente Reglamento, los tribunales nacionales que estimen necesaria una decisión al respecto para poder emitir su fallo pueden, o en el caso establecido en el artículo 267 del TFUE, deben solicitar al Tribunal de Justicia que se pronuncie con carácter prejudicial sobre la interpretación del Derecho de la Unión, incluido el presente Reglamento. Además, si una decisión de una autoridad de control por la que se ejecuta una decisión del Comité se impugna ante un tribunal nacional y se cuestiona la validez de la decisión del Comité, dicho tribunal nacional no es competente para declarar inválida la decisión del Comité, sino que, si la considera inválida, tiene que remitir la cuestión de la validez al Tribunal de Justicia de conformidad con el artículo 267 del TFUE, según la interpretación de este. No obstante, un tribunal nacional puede no remitir la cuestión de la validez de la decisión del Comité a instancia de una persona física o jurídica que, habiendo tenido la oportunidad de interponer recurso de anulación de dicha decisión, en particular si dicha decisión la afectaba directa e individualmente, no lo hizo en el plazo establecido en el artículo 263 del TFUE.

(144) Si un tribunal ante el cual se ejercitaron acciones contra una decisión de una autoridad de control tiene motivos para creer que se ejercitaron acciones ante un tribunal competente de otro Estado miembro relativas al mismo tratamiento, como tener el mismo asunto con respecto a un tratamiento por el mismo responsable o encargado, o la misma causa de la acción, debe ponerse en contacto con ese tribunal para confirmar la existencia de tales acciones conexas. Si dichas acciones conexas están pendientes ante un tribunal de otro Estado miembro, cualquier otro tribunal distinto de aquel ante el cual se ejercitó la acción en primer lugar puede suspender el procedimiento o, a instancia de una de las partes, inhibirse a favor del tribunal ante el cual se ejercitó la acción en primer lugar si este último es competente para su conocimiento y su acumulación es conforme a Derecho. Se consideran conexas las acciones vinculadas entre sí por una relación tan estrecha que procede tramitarlas y resolverlas conjuntamente a fin de evitar resoluciones que podrían ser incompatibles si se sustanciaran como causas separadas.

(145) Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

(146) El responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento. El responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que en modo alguno son responsables de los daños y perjuicios. El concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos del presente Reglamento. Lo anterior se entiende sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros. Un tratamiento en infracción del presente Reglamento también incluye aquel tratamiento que infringe actos delegados y de ejecución adoptados de conformidad con el presente Reglamento y el Derecho de los Estados miembros que especifique las normas del presente Reglamento. Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos. Si los responsables o encargados participan en el mismo tratamiento, cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios. No obstante, si se acumulan en la misma causa de conformidad con el Derecho de los Estados miembros, la indemnización puede prorratearse en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, siempre

que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios. Todo responsable o encargado que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables o encargados que hayan participado en el mismo tratamiento.

(147) En los casos en que el presente Reglamento contiene normas específicas sobre competencia judicial, en particular por lo que respecta a las acciones que tratan de obtener satisfacción por la vía judicial, incluida la indemnización, contra un responsable o encargado del tratamiento, las normas generales de competencia judicial como las establecidas en el Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo [13] deben entenderse sin perjuicio de la aplicación de dichas normas específicas.

(148) A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

(149) Los Estados miembros deben tener la posibilidad de establecer normas en materia de sanciones penales por infracciones del presente Reglamento, incluidas las infracciones de normas nacionales adoptadas con arreglo a él y dentro de sus límites. Dichas sanciones penales pueden asimismo autorizar la privación de los beneficios obtenidos en infracción del presente Reglamento. No obstante, la imposición de sanciones penales por infracciones de dichas normas nacionales y de sanciones administrativas no debe entrañar la vulneración del principio ne bis in idem, según la interpretación del Tribunal de Justicia.

(150) A fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, cada autoridad de control debe estar facultada para imponer multas administrativas. El presente Reglamento debe indicar las infracciones así como el límite máximo y los criterios para fijar las correspondientes multas administrativas, que la autoridad de control competente debe determinar en cada caso individual teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo en particular a la naturaleza, gravedad y duración de la infracción y sus consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o mitigar las consecuencias de la infracción. Si las multas administrativas se imponen a una empresa, por tal debe entenderse una empresa con arreglo a los artículos 101 y 102 del TFUE. Si las multas administrativas se imponen a personas que no son una empresa, la autoridad de control debe tener en cuenta al valorar la cuantía apropiada de la multa el nivel general de ingresos prevaleciente en el Estado miembro así como la situación económica de la persona. El mecanismo de coherencia también puede emplearse para fomentar una aplicación coherente de las multas administrativas. Debe corresponder a los Estados miembros determinar si y en qué medida se debe imponer multas administrativas a las autoridades públicas. La imposición de una multa administrativa o de una advertencia no afecta al ejercicio de otras competencias de las autoridades de control ni a la aplicación de otras sanciones al amparo del presente Reglamento.

(151) Los ordenamientos jurídicos de Dinamarca y Estonia no permiten las multas administrativas según lo dispuesto en el presente Reglamento. Las normas sobre multas administrativas pueden ser aplicadas en Dinamarca de tal manera que la multa sea impuesta por los tribunales nacionales competentes en cuanto sanción penal, y en Estonia de tal manera que la multa sea impuesta por la autoridad de control en el marco de un juicio de faltas, siempre que tal aplicación de las normas en dichos Estados miembros tenga un efecto

equivalente a las multas administrativas impuestas por las autoridades de control. Por lo tanto los tribunales nacionales competentes deben tener en cuenta la recomendación de la autoridad de control que incoe la multa. En todo caso, las multas impuestas deben ser efectivas, proporcionadas y disuasorias.

(152) En los casos en que el presente Reglamento no armoniza las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en casos de infracciones graves del presente Reglamento, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. La naturaleza de dichas sanciones, ya sea penal o administrativa, debe ser determinada por el Derecho de los Estados miembros.

(153) El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio.

(154) El presente Reglamento permite que, al aplicarlo, se tenga en cuenta el principio de acceso del público a los documentos oficiales. El acceso del público a documentos oficiales puede considerarse de interés público. Los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el Derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo. Ambos Derechos deben conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales y, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el presente Reglamento. La referencia a autoridades y organismos públicos debe incluir, en este contexto, a todas las autoridades u otros organismos a los que se aplica el Derecho de los Estados miembros sobre el acceso del público a documentos. La Directiva 2003/98/CE del Parlamento Europeo y del Consejo [(14)] no altera ni afecta en modo alguno al nivel de protección de las personas físicas con respecto al tratamiento de datos personales con arreglo a las disposiciones del Derecho de la Unión y los Estados miembros y, en particular, no altera las obligaciones ni los derechos establecidos en el presente Reglamento. En concreto, dicha Directiva no debe aplicarse a los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de datos personales, ni a partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización haya quedado establecida por ley como incompatible con el Derecho relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales.

(155) El Derecho de los Estados miembros o los convenios colectivos, incluidos los «convenios de empresa», pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la

ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral.

(156) El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y libertades del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos. El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos). Los Estados miembros deben establecer garantías adecuadas para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Debe autorizarse que los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos.

(157) Combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros.

(158) El presente Reglamento también debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no debe se de aplicación a personas fallecidas. Las autoridades públicas o los organismos públicos o privados que llevan registros de interés público deben ser servicios que están obligados, con arreglo al Derecho de la Unión o de los Estados miembros, a adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros de valor perdurable para el interés público general y facilitar acceso a ellos. Los Estados miembros también debe estar autorizados a establecer el tratamiento ulterior de datos personales con fines de archivo, por ejemplo a fin de ofrecer información específica relacionada con el comportamiento político bajo antiguos regímenes de Estados totalitarios, el genocidio, los crímenes contra la humanidad, en particular el Holocausto, o los crímenes de guerra.

(159) El presente Reglamento también debe aplicarse al tratamiento datos personales que se realice con fines de investigación científica. El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de

manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas.

(160) El presente Reglamento debe aplicarse asimismo al tratamiento datos personales que se realiza con fines de investigación histórica. Esto incluye asimismo la investigación histórica y la investigación para fines genealógicos, teniendo en cuenta que el presente Reglamento no es de aplicación a personas fallecidas.

(161) Al objeto de otorgar el consentimiento para la participación en actividades de investigación científica en ensayos clínicos, deben aplicarse las disposiciones pertinentes del Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo [(15)].

(162) El presente Reglamento debe aplicarse al tratamiento de datos personales con fines estadísticos. El contenido estadístico, el control de accesos, las especificaciones para el tratamiento de datos personales con fines estadísticos y las medidas adecuadas para salvaguardar los derechos y las libertades de los interesados y garantizar la confidencialidad estadística deben ser establecidos, dentro de los límites del presente Reglamento, por el Derecho de la Unión o de los Estados miembros. Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos. Estos resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica. El fin estadístico implica que el resultado del tratamiento con fines estadísticos no sean datos personales, sino datos agregados, y que este resultado o los datos personales no se utilicen para respaldar medidas o decisiones relativas a personas físicas concretas.

(163) Debe protegerse la información confidencial que las autoridades estadísticas de la Unión y nacionales recojan para la elaboración de las estadísticas oficiales europeas y nacionales. Las estadísticas europeas deben desarrollarse, elaborarse y difundirse con arreglo a los principios estadísticos fijados en el artículo 338, apartado 2, del TFUE, mientras que las estadísticas nacionales deben cumplir asimismo el Derecho de los Estados miembros. El Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo [(16)] facilita especificaciones adicionales sobre la confidencialidad estadística aplicada a las estadísticas europeas.

(164) Por lo que respecta a los poderes de las autoridades de control para obtener del responsable o del encargado del tratamiento acceso a los datos personales y a sus locales, los Estados miembros pueden adoptar por ley, dentro de los límites fijados por el presente Reglamento, normas específicas con vistas a salvaguardar el deber de secreto profesional u obligaciones equivalentes, en la medida necesaria para conciliar el derecho a la protección de los datos personales con el deber de secreto profesional. Lo anterior se entiende sin perjuicio de las obligaciones existentes para los Estados miembros de adoptar normas sobre el secreto profesional cuando así lo exija el Derecho de la Unión.

(165) El presente Reglamento respeta y no prejuzga el estatuto reconocido en los Estados miembros, en virtud del Derecho constitucional, a las iglesias y las asociaciones o comunidades religiosas, tal como se reconoce en el artículo 17 del TFUE.

(166) A fin de cumplir los objetivos del presente Reglamento, a saber, proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y garantizar la libre circulación de los datos personales en la Unión, debe delegarse en la Comisión el poder de adoptar actos de conformidad con el artículo 290 del TFUE. En particular, deben adoptarse actos delegados en relación con los criterios y requisitos para los mecanismos de certificación, la información que debe presentarse mediante iconos normalizados y los procedimientos para proporcionar

dichos iconos. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. Al preparar y redactar los actos delegados, la Comisión debe garantizar la transmisión simultánea, oportuna y apropiada de los documentos pertinentes al Parlamento Europeo y al Consejo.

(167) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución cuando así lo establezca el presente Reglamento. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo. En este contexto, la Comisión debe considerar la adopción de medidas específicas para las microempresas y las pequeñas y medianas empresas.

(168) El procedimiento de examen debe seguirse para la adopción de actos de ejecución sobre cláusulas contractuales tipo entre responsables y encargados del tratamiento y entre responsables del tratamiento; códigos de conducta; normas técnicas y mecanismos de certificación; el nivel adecuado de protección ofrecido por un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional; cláusulas tipo de protección; formatos y procedimientos para el intercambio de información entre responsables, encargados y autoridades de control respecto de normas corporativas vinculantes; asistencia mutua; y modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre las autoridades de control y el Comité.

(169) La Comisión debe adoptar actos de ejecución inmediatamente aplicables cuando las pruebas disponibles muestren que un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional no garantizan un nivel de protección adecuado y así lo requieran razones imperiosas de urgencia.

(170) Dado que el objetivo del presente Reglamento, a saber, garantizar un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones o los efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(171) La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Todo tratamiento ya iniciado en la fecha de aplicación del presente Reglamento debe ajustarse al presente Reglamento en el plazo de dos años a partir de la fecha de su entrada en vigor. Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento. Las decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas.

(172) De conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001, se consultó al Supervisor Europeo de Protección de Datos, y éste emitió su dictamen el 7 de marzo de 2012 [17].

(173) El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo [18], incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas. Para aclarar la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia. Una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento.

HAN ADOPTADO EL PRESENTE REGLAMENTO

---

(1) DO C 229 de 31.7.2012, p. 90.

(2) DO C 391 de 18.12.2012, p. 127.

(3) Posición del Parlamento Europeo de 12 de marzo de 2014 (pendiente de publicación en el Diario Oficial) y posición del Consejo en primera lectura de 8 de abril de 2016 (pendiente de publicación en el Diario Oficial). Posición del Parlamento Europeo de 14 de abril de 2016.

(4) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

(5) Recomendación de la Comisión de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas [C(2003) 1422] (DO L 124 de 20.5.2003, p. 36).

(6) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

(7) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (véase la página 89 del presente Diario Oficial).

(8) Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000, p. 1).

(9) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

(10) Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95 de 21.4.1993, p. 29).

(11) Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo (DO L 354 de 31.12.2008, p. 70).

(12) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(13) Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DO L 351 de 20.12.2012, p. 1).

(14) Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público (DO L 345 de 31.12.2003, p. 90).

(15) Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE (DO L 158 de 27.5.2014, p. 1).

(16) Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008 relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) n.º 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas (DO L 87 de 31.3.2009, p. 164).

(17) DO C 192 de 30.6.2012, p. 7.

(18) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Artículo 2. *Ámbito de aplicación material.*

1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

3. El Reglamento (CE) n.º 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.

4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

Artículo 3. *Ámbito territorial.*

1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

Artículo 4. *Definiciones.*

A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o

cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

16) «establecimiento principal»:

a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las

decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c) se ha presentado una reclamación ante esa autoridad de control;

23) «tratamiento transfronterizo»:

a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo [(19)];

26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

---

(19) Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

CAPÍTULO II

Principios

Artículo 5. *Principios relativos al tratamiento.*

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 6. *Licitud del tratamiento.*

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no

prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Artículo 7. *Condiciones para el consentimiento.*

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el

consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 8. *Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.*

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Artículo 9. *Tratamiento de categorías especiales de datos personales.*

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 10. *Tratamiento de datos personales relativos a condenas e infracciones penales.*

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 11. *Tratamiento que no requiere identificación.*

1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

CAPÍTULO III

Derechos del interesado

Sección 1. Transparencia y modalidades

Artículo 12. *Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.*

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, sin dilación indebida y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Sección 2. Información y acceso a los datos personales

Artículo 13. *Información que deberá facilitarse cuando los datos personales se obtengan del interesado.*

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;
f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14. *Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.*

1. Cuando los datos personales no se hayan obtenido del interesado, el responsable del tratamiento le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;

c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;

b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o

c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza legal.

Artículo 15. *Derecho de acceso del interesado.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros países u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Sección 3. Rectificación y supresión

Artículo 16. *Derecho de rectificación.*

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 17. *Derecho de supresión («el derecho al olvido»).*

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18. *Derecho a la limitación del tratamiento.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales en un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19. *Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.*

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20. *Derecho a la portabilidad de los datos.*

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Sección 4. Derecho de oposición y decisiones individuales automatizadas

Artículo 21. *Derecho de oposición.*

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22. *Decisiones individuales automatizadas, incluida la elaboración de perfiles.*

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Sección 5. Limitaciones

Artículo 23. *Limitaciones.*

1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;

b) las categorías de datos personales de que se trate;

c) el alcance de las limitaciones establecidas;

d) las garantías para evitar accesos o transferencias ilícitos o abusivos;

e) la determinación del responsable o de categorías de responsables;

f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza, alcance y objetivos del tratamiento o las categorías de tratamiento;

g) los riesgos para los derechos y libertades de los interesados, y

h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

CAPÍTULO IV

Responsable del tratamiento y encargado del tratamiento

Sección 1. Obligaciones generales

Artículo 24. *Responsabilidad del responsable del tratamiento.*

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Artículo 25. *Protección de datos desde el diseño y por defecto.*

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Artículo 26. *Corresponsables del tratamiento.*

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados

miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Artículo 27. *Representantes de responsables o encargados del tratamiento no establecidos en la Unión.*

1. Cuando sea de aplicación el artículo 3, apartado 2, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión.

2. La obligación establecida en el apartado 1 del presente artículo no será aplicable:

a) al tratamiento que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o

b) a las autoridades u organismos públicos.

3. El representante estará establecido en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado.

4. El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en el presente Reglamento.

5. La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Artículo 28. *Encargado del tratamiento.*

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 29. *Tratamiento bajo la autoridad del responsable o del encargado del tratamiento.*

El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 30. *Registro de las actividades de tratamiento.*

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.
4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.
5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 31. *Cooperación con la autoridad de control.*

El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

Sección 2. Seguridad de los datos personales

Artículo 32. *Seguridad del tratamiento.*

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.
4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 33. *Notificación de una violación de la seguridad de los datos personales a la autoridad de control.*

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34. *Comunicación de una violación de la seguridad de los datos personales al interesado.*

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa

Artículo 35. *Evaluación de impacto relativa a la protección de datos.*

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 36. *Consulta previa.*

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no

haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d) en su caso, los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control.

4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

Sección 4. Delegado de protección de datos

Artículo 37. *Designación del delegado de protección de datos.*

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9 o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 38. *Posición del delegado de protección de datos.*

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Artículo 39. *Funciones del delegado de protección de datos.*

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Sección 5. Códigos de conducta y certificación

Artículo 40. *Códigos de conducta.*

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:

a) el tratamiento leal y transparente;

b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;

c) la recogida de datos personales;

d) la seudonimización de datos personales;

e) la información proporcionada al público y a los interesados;

f) el ejercicio de los derechos de los interesados;

g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;

h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;

i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;

j) la transferencia de datos personales a terceros países u organizaciones internacionales, o

k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

3. Además de la adhesión de los responsables o encargados del tratamiento a los que se aplica el presente Reglamento, los responsables o encargados a los que no se aplica el presente Reglamento en virtud del artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el apartado 5 del presente artículo y que tengan validez general en virtud del apartado 9 del presente artículo, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra e). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

4. El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apartado 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 51 o 56.

5. Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al artículo 55. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.

6. Si el proyecto de código o la modificación o ampliación es aprobado de conformidad con el apartado 5 y el código de conducta de que se trate no se refiere a actividades de

tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código.

7. Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente en virtud del artículo 55 lo presentará por el procedimiento mencionado en el artículo 63, antes de su aprobación o de la modificación o ampliación, al Comité, el cual dictaminará si dicho proyecto, modificación o ampliación es conforme con el presente Reglamento o, en la situación indicada en el apartado 3 del presente artículo, ofrece garantías adecuadas.

8. Si el dictamen a que se refiere el apartado 7 confirma que el proyecto de código o la modificación o ampliación cumple lo dispuesto en el presente Reglamento o, en la situación indicada en el apartado 3, ofrece garantías adecuadas, el Comité presentará su dictamen a la Comisión.

9. La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados con arreglo al apartado 8 del presente artículo tengan validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

10. La Comisión dará publicidad adecuada a los códigos aprobados cuya validez general haya sido decidida de conformidad con el apartado 9.

11. El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 41. *Supervisión de códigos de conducta aprobados.*

1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.

2. El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:

a) ha demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código;

b) ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;

c) ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

d) ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los requisitos de acreditación de un organismo a que se refiere el apartado 1 del presente artículo.

4. Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.

5. La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si los requisitos de acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento.

6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.

Artículo 42. *Certificación.*

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

3. La certificación será voluntaria y estará disponible a través de un proceso transparente.

4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56.

5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.

6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.

7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los criterios pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los criterios para la certificación.

8. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 43. *Organismo de certificación.*

1. Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos:

a) la autoridad de control que sea competente en virtud del artículo 55 o 56;

b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo [20] con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56.

2. Los organismos de certificación mencionados en el apartado 1 únicamente serán acreditados de conformidad con dicho apartado si:

a) han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación;

b) se han comprometido a respetar los criterios mencionados en el artículo 42, apartado 5, y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63;

c) han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos;

d) han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

e) han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La acreditación de los organismos de certificación a que se refieren los apartados 1 y 2 del presente artículo se realizará sobre la base de los requisitos aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56 o por el Comité en virtud del artículo 63. En caso de acreditación de conformidad con el apartado 1, letra b), del presente artículo, estos requisitos complementarán los contemplados en el Reglamento (CE) n.º 765/2008 y las normas técnicas que describen los métodos y procedimientos de los organismos de certificación.

4. Los organismos de certificación a que se refiere el apartado 1 serán responsable de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del presente Reglamento. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el presente artículo.

5. Los organismos de certificación a que se refiere el apartado 1 comunicarán a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada.

6. La autoridad de control hará públicos los requisitos a que se refiere el apartado 3 del presente artículo y los criterios a que se refiere el artículo 42, apartado 5, en una forma fácilmente accesible. Las autoridades de control comunicarán también dichos requisitos y criterios al Comité.

7. No obstante lo dispuesto en el capítulo VIII, la autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación a tenor del apartado 1 del presente artículo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el presente Reglamento.

8. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 92, a fin de especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos a que se refiere el artículo 42, apartado 1.

9. La Comisión podrá adoptar actos de ejecución que establezcan normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, y mecanismos para promover y reconocer dichos mecanismos de certificación, sellos y marcas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

---

[20] Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

CAPÍTULO V

Transferencias de datos personales a terceros países u organizaciones internacionales

Artículo 44. *Principio general de las transferencias.*

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 45. *Transferencias basadas en una decisión de adecuación.*

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las

decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.

6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

Artículo 46. *Transferencias mediante garantías adecuadas.*

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) normas corporativas vinculantes de conformidad con el artículo 47;

c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 47. *Normas corporativas vinculantes.*

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 48. *Transferencias o comunicaciones no autorizadas por el Derecho de la Unión.*

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

Artículo 49. *Excepciones para situaciones específicas.*

1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Artículo 50. *Cooperación internacional en el ámbito de la protección de datos personales.*

En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:

a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales;

b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;

c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

CAPÍTULO VI

Autoridades de control independientes

Sección 1. Independencia

Artículo 51. *Autoridad de control.*

1. Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII.

3. Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63.

4. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el presente capítulo a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que afecte a dichas disposiciones.

Artículo 52. *Independencia.*

1. Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento.

2. El miembro o los miembros de cada autoridad de control serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.

3. El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité.

5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada.

6. Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

Artículo 53. *Condiciones generales aplicables a los miembros de la autoridad de control.*

1. Los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente por:

— su Parlamento,
— su Gobierno,
— su Jefe de Estado, o
— un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros.

2. Cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

3. Los miembros darán por concluidas sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria, de conformidad con el Derecho del Estado miembro de que se trate.

4. Un miembro será destituido únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones.

Artículo 54. *Normas relativas al establecimiento de la autoridad de control.*

1. Cada Estado miembro establecerá por ley todos los elementos indicados a continuación:

a) el establecimiento de cada autoridad de control;

b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control;

c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;

d) la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado;

e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;

f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.

2. El miembro o miembros y el personal de cada autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento.

Sección 2. Competencia, funciones y poderes

Artículo 55. *Competencia.*

1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro.

2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el artículo 56.

3. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

Artículo 56. *Competencia de la autoridad de control principal.*

1. Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

2. No obstante lo dispuesto en el apartado 1, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro.

3. En los casos a que se refiere el apartado 2 del presente artículo, la autoridad de control informará sin dilación al respecto a la autoridad de control principal. En el plazo de tres semanas después de haber sido informada, la autoridad de control principal decidirá si tratará o no el caso de conformidad con el procedimiento establecido en el artículo 60, teniendo presente si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado.

4. En caso de que la autoridad de control principal decida tratar el caso, se aplicará el procedimiento establecido en el artículo 60. La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión. La autoridad de control principal tendrá en cuenta en la mayor medida posible dicho proyecto al preparar el proyecto de decisión a que se refiere el artículo 60, apartado 3.

5. En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará con arreglo a los artículos 61 y 62.

6. La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado.

Artículo 57. *Funciones.*

1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

a) controlar la aplicación del presente Reglamento y hacerlo aplicar;

b) promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención;

c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;

d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento;

e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;

f) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

g) cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento;

h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;

i) hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;

j) adoptar las cláusulas contractuales tipo a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

k) elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4;

l) ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2;

m) alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5;

n) fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5;

o) llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas en virtud del artículo 42, apartado 7;

p) elaborar y publicar los requisitos para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

q) efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

r) autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3;

s) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47;

t) contribuir a las actividades del Comité;

u) llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2, y

v) desempeñar cualquier otra función relacionada con la protección de los datos personales.

2. Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

3. El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Artículo 58. *Poderes.*

1. Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación:

a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;

b) llevar a cabo investigaciones en forma de auditorías de protección de datos;

c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

a) dirigir a todo responsable o encargado del tratamiento una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;

h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

3. Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;

b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;

d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5;

e) acreditar los organismos de certificación con arreglo al artículo 43;

f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;

g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);

i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);

j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.

4. El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.

5. Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.

6. Cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del capítulo VII.

Artículo 59. *Informe de actividad.*

Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité.

CAPÍTULO VII

Cooperación y coherencia

Sección 1. Cooperación y coherencia

Artículo 60. *Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas.*

1. La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente.

2. La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.

3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.

4. En caso de que cualquiera de las autoridades de control interesadas formule una objeción pertinente y motivada acerca del proyecto de decisión en un plazo de cuatro semanas a partir de la consulta con arreglo al apartado 3 del presente artículo, la autoridad de control principal someterá el asunto, en caso de que no siga lo indicado en la objeción pertinente y motivada o estime que dicha objeción no es pertinente o no está motivada, al mecanismo de coherencia contemplado en el artículo 63.

5. En caso de que la autoridad de control principal prevea seguir lo indicado en la objeción pertinente y motivada recibida, presentará a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado. Dicho proyecto de decisión revisado se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas.

6. En caso de que ninguna otra autoridad de control interesada haya presentado objeciones al proyecto de decisión transmitido por la autoridad de control principal en el plazo indicado en los apartados 4 y 5, se considerará que la autoridad de control principal y

las autoridades de control interesadas están de acuerdo con dicho proyecto de decisión y estarán vinculadas por este.

7. La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante.

8. No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento.

9. En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado.

10. Tras recibir la notificación de la decisión de la autoridad de control principal con arreglo a los apartados 7 y 9, el responsable o el encargado del tratamiento adoptará las medidas necesarias para garantizar el cumplimiento de la decisión en lo tocante a las actividades de tratamiento en el contexto de todos sus establecimientos en la Unión. El responsable o el encargado notificarán las medidas adoptadas para dar cumplimiento a dicha decisión a la autoridad de control principal, que a su vez informará a las autoridades de control interesadas.

11. En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66.

12. La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado.

Artículo 61. *Asistencia mutua.*

1. Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua a fin de aplicar el presente Reglamento de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones.

2. Cada autoridad de control adoptará todas las medidas oportunas requeridas para responder a una solicitud de otra autoridad de control sin dilación indebida y a más tardar en el plazo de un mes a partir de la solicitud. Dichas medidas podrán incluir, en particular, la transmisión de información pertinente sobre el desarrollo de una investigación.

3. Las solicitudes de asistencia deberán contener toda la información necesaria, entre otras cosas respecto de la finalidad y los motivos de la solicitud. La información que se intercambie se utilizará únicamente para el fin para el que haya sido solicitada.

4. La autoridad de control requerida no podrá negarse a responder a una solicitud, salvo si:

a) no es competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita, o

b) el hecho de responder a la solicitud infringiría el presente Reglamento o el Derecho de la Unión o de los Estados miembros que se aplique a la autoridad de control a la que se dirigió la solicitud.

5. La autoridad de control requerida informará a la autoridad de control requirente de los resultados obtenidos o, en su caso, de los progresos registrados o de las medidas

adoptadas para responder a su solicitud. La autoridad de control requerida explicará los motivos de su negativa a responder a una solicitud al amparo del apartado 4.

6. Como norma general, las autoridades de control requeridas facilitarán la información solicitada por otras autoridades de control por medios electrónicos, utilizando un formato normalizado.

7. Las autoridades de control requeridas no cobrarán tasa alguna por las medidas adoptadas a raíz de una solicitud de asistencia mutua. Las autoridades de control podrán convenir normas de indemnización recíproca por gastos específicos derivados de la prestación de asistencia mutua en circunstancias excepcionales.

8. Cuando una autoridad de control no facilite la información mencionada en el apartado 5 del presente artículo en el plazo de un mes a partir de la recepción de la solicitud de otra autoridad de control, la autoridad de control requirente podrá adoptar una medida provisional en el territorio de su Estado miembro de conformidad con lo dispuesto en el artículo 55, apartado 1. En ese caso, se supondrá que existe la necesidad urgente contemplada en el artículo 66, apartado 1, que exige una decisión urgente y vinculante del Comité en virtud del artículo 66, apartado 2.

9. La Comisión podrá, mediante actos de ejecución, especificar el formato y los procedimientos de asistencia mutua contemplados en el presente artículo, así como las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité, en especial el formato normalizado mencionado en el apartado 6 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 62. *Operaciones conjuntas de las autoridades de control.*

1. Las autoridades de control realizarán, en su caso, operaciones conjuntas, incluidas investigaciones conjuntas y medidas de ejecución conjuntas, en las que participen miembros o personal de las autoridades de control de otros Estados miembros.

2. Si el responsable o el encargado del tratamiento tiene establecimientos en varios Estados miembros o si es probable que un número significativo de interesados en más de un Estado miembro se vean sustancialmente afectados por las operaciones de tratamiento, una autoridad de control de cada uno de esos Estados miembros tendrá derecho a participar en operaciones conjuntas. La autoridad de control que sea competente en virtud del artículo 56, apartados 1 o 4, invitará a la autoridad de control de cada uno de dichos Estados miembros a participar en las operaciones conjuntas y responderá sin dilación a la solicitud de participación presentada por una autoridad de control.

3. Una autoridad de control podrá, con arreglo al Derecho de su Estado miembro y con la autorización de la autoridad de control de origen, conferir poderes, incluidos poderes de investigación, a los miembros o al personal de la autoridad de control de origen que participen en operaciones conjuntas, o aceptar, en la medida en que lo permita el Derecho del Estado miembro de la autoridad de control de acogida, que los miembros o el personal de la autoridad de control de origen ejerzan sus poderes de investigación de conformidad con el Derecho del Estado miembro de la autoridad de control de origen. Dichos poderes de investigación solo podrán ejercerse bajo la orientación y en presencia de miembros o personal de la autoridad de control de acogida. Los miembros o el personal de la autoridad de control de origen estarán sujetos al Derecho del Estado miembro de la autoridad de control de acogida.

4. Cuando participe, de conformidad con el apartado 1, personal de la autoridad de control de origen en operaciones en otro Estado miembro, el Estado miembro de la autoridad de control de acogida asumirá la responsabilidad de acuerdo con el Derecho del Estado miembro en cuyo territorio se desarrollen las operaciones, por los daños y perjuicios que haya causado dicho personal en el transcurso de las mismas.

5. El Estado miembro en cuyo territorio se causaron los daños y perjuicios asumirá su reparación en las condiciones aplicables a los daños y perjuicios causados por su propio personal. El Estado miembro de la autoridad de control de origen cuyo personal haya causado daños y perjuicios a cualquier persona en el territorio de otro Estado miembro le restituirá íntegramente los importes que este último haya abonado a los derechohabientes.

6. Sin perjuicio del ejercicio de sus derechos frente a terceros y habida cuenta de la excepción establecida en el apartado 5, los Estados miembros renunciarán, en el caso contemplado en el apartado 1, a solicitar de otro Estado miembro el reembolso del importe de los daños y perjuicios mencionados en el apartado 4.

7. Cuando se prevea una operación conjunta y una autoridad de control no cumpla en el plazo de un mes con la obligación establecida en el apartado 2, segunda frase, del presente artículo, las demás autoridades de control podrán adoptar una medida provisional en el territorio de su Estado miembro de conformidad con el artículo 55. En ese caso, se presumirá la existencia de una necesidad urgente a tenor del artículo 66, apartado 1, y se requerirá dictamen o decisión vinculante urgente del Comité en virtud del artículo 66, apartado 2.

Sección 2. Coherencia

Artículo 63. *Mecanismo de coherencia.*

A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección.

Artículo 64. *Dictamen del Comité.*

1. El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión:

a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;

b) afecte a un asunto de conformidad con el artículo 40, apartado 7, cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento;

c) tenga por objeto aprobar los requisitos para la acreditación de un organismo con arreglo al artículo 41, apartado 3, de un organismo de certificación conforme al artículo 43, apartado 3, o los criterios aplicables a la certificación a que se refiere el artículo 42, apartado 5;

d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, letra d), y el artículo 28, apartado 8;

e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, letra a);

f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del artículo 47.

2. Cualquier autoridad de control, el presidente del Comité o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61 o las operaciones conjuntas con arreglo al artículo 62.

3. En los casos a que se refieren los apartados 1 y 2, el Comité emitirá dictamen sobre el asunto que le haya sido presentado siempre que no haya emitido ya un dictamen sobre el mismo asunto. Dicho dictamen se adoptará en el plazo de ocho semanas por mayoría simple de los miembros del Comité. Dicho plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Por lo que respecta al proyecto de decisión a que se refiere el apartado 1 y distribuido a los miembros del Comité con arreglo al apartado 5, todo miembro que no haya presentado objeciones dentro de un plazo razonable indicado por el presidente se considerará conforme con el proyecto de decisión.

4. Las autoridades de control y la Comisión comunicarán sin dilación por vía electrónica al Comité, utilizando un formato normalizado, toda información útil, en particular, cuando proceda, un resumen de los hechos, el proyecto de decisión, los motivos por los que es necesaria tal medida, y las opiniones de otras autoridades de control interesadas.

5. La Presidencia del Comité informará sin dilación indebida por medios electrónicos:

a) a los miembros del Comité y a la Comisión de cualquier información pertinente que le haya sido comunicada, utilizando un formato normalizado. La secretaría del Comité facilitará, de ser necesario, traducciones de la información que sea pertinente, y

b) a la autoridad de control contemplada, en su caso, en los apartados 1 y 2 y a la Comisión del dictamen, y lo publicará.

6. La autoridad de control competente a que se refiere el apartado 1 no adoptará su proyecto de decisión a tenor del apartado 1 en el plazo mencionado en el apartado 3.

7. La autoridad de control competente a que se refiere el apartado 1 tendrá en cuenta en la mayor medida posible el dictamen del Comité y, en el plazo de dos semanas desde la recepción del dictamen, comunicará por medios electrónicos al presidente del Comité si va a mantener o modificar su proyecto de decisión y, si lo hubiera, el proyecto de decisión modificado, utilizando un formato normalizado.

8. Cuando la autoridad de control competente a que se refiere el apartado 1 informe al presidente del Comité, en el plazo mencionado en el apartado 7 del presente artículo, de que no prevé seguir el dictamen del Comité, en todo o en parte, alegando los motivos correspondientes, se aplicará el artículo 65, apartado 1.

Artículo 65. *Resolución de conflictos por el Comité.*

1. Con el fin de garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante en los siguientes casos:

a) cuando, en un caso mencionado en el artículo 60, apartado 4, una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad de control principal y esta no haya seguido la objeción o haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos a que se refiera la objeción pertinente y motivada, en particular si hay infracción del presente Reglamento;

b) cuando haya puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal;

c) cuando una autoridad de control competente no solicite dictamen al Comité en los casos contemplados en el artículo 64, apartado 1, o no siga el dictamen del Comité emitido en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, lo pondrá en conocimiento del Comité.

2. La decisión a que se refiere el apartado 1 se adoptará en el plazo de un mes a partir de la remisión del asunto, por mayoría de dos tercios de los miembros del Comité. Este plazo podrá prorrogarse un mes más, habida cuenta de la complejidad del asunto. La decisión que menciona el apartado 1 estará motivada y será dirigida a la autoridad de control principal y a todas las autoridades de control interesadas, y será vinculante para ellas.

3. Cuando el Comité no haya podido adoptar una decisión en los plazos mencionados en el apartado 2, adoptará su decisión en un plazo de dos semanas tras la expiración del segundo mes a que se refiere el apartado 2, por mayoría simple de sus miembros. En caso de empate, decidirá el voto del presidente.

4. Las autoridades de control interesadas no adoptarán decisión alguna sobre el asunto presentado al Comité en virtud del apartado 1 durante los plazos de tiempo a que se refieren los apartados 2 y 3.

5. El presidente del Comité notificará sin dilación indebida la decisión contemplada en el apartado 1 a las autoridades de control interesadas. También informará de ello a la Comisión. La decisión se publicará en el sitio web del Comité sin demora, una vez que la autoridad de control haya notificado la decisión definitiva a que se refiere el apartado 6.

6. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de la decisión contemplada en el apartado 1 del presente artículo, sin dilación indebida y a más tardar un mes tras la notificación de la decisión del Comité. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación informará al Comité de la fecha de notificación de su decisión definitiva al responsable o al encargado del

tratamiento y al interesado, respectivamente. La decisión definitiva de las autoridades de control interesadas será adoptada en los términos establecidos en el artículo 60, apartados 7, 8 y 9. La decisión definitiva hará referencia a la decisión contemplada en el apartado 1 del presente artículo y especificará que esta última decisión se publicará en el sitio web del Comité con arreglo al apartado 5 del presente artículo. La decisión definitiva llevará adjunta la decisión contemplada en el apartado 1 del presente artículo.

Artículo 66. *Procedimiento de urgencia.*

1. En circunstancias excepcionales, cuando una autoridad de control interesada considere que es urgente intervenir para proteger los derechos y las libertades de interesados, podrá, como excepción al mecanismo de coherencia contemplado en los artículos 63, 64 y 65, o al procedimiento mencionado en el artículo 60, adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un periodo de validez determinado que no podrá ser superior a tres meses. La autoridad de control comunicará sin dilación dichas medidas, junto con los motivos de su adopción, a las demás autoridades de control interesadas, al Comité y a la Comisión.

2. Cuando una autoridad de control haya adoptado una medida de conformidad con el apartado 1, y considere que deben adoptarse urgentemente medidas definitivas, podrá solicitar con carácter urgente un dictamen o una decisión vinculante urgente del Comité, motivando dicha solicitud de dictamen o decisión.

3. Cualquier autoridad de control podrá solicitar, motivando su solicitud, y, en particular, la urgencia de la intervención, un dictamen urgente o una decisión vinculante urgente, según el caso, del Comité, cuando una autoridad de control competente no haya tomado una medida apropiada en una situación en la que sea urgente intervenir a fin de proteger los derechos y las libertades de los interesados.

4. No obstante lo dispuesto en el artículo 64, apartado 3, y en el artículo 65, apartado 2, los dictámenes urgentes o decisiones vinculantes urgentes contemplados en los apartados 2 y 3 del presente artículo se adoptarán en el plazo de dos semanas por mayoría simple de los miembros del Comité.

Artículo 67. *Intercambio de información.*

La Comisión podrá adoptar actos de ejecución de ámbito general para especificar las modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre dichas autoridades y el Comité, en especial el formato normalizado contemplado en el artículo 64.

Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Sección 3. Comité europeo de protección de datos

Artículo 68. *Comité Europeo de Protección de Datos.*

1. Se crea el Comité Europeo de Protección de Datos («Comité»), como organismo de la Unión, que gozará de personalidad jurídica.

2. El Comité estará representado por su presidente.

3. El Comité estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos.

4. Cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro.

5. La Comisión tendrá derecho a participar en las actividades y reuniones del Comité, sin derecho a voto. La Comisión designará un representante. El presidente del Comité comunicará a la Comisión las actividades del Comité.

6. En los casos a que se refiere el artículo 65, el Supervisor Europeo de Protección de Datos sólo tendrá derecho a voto en las decisiones relativas a los principios y normas

aplicables a las instituciones, órganos y organismos de la Unión que correspondan en cuanto al fondo a las contempladas en el presente Reglamento.

Artículo 69. *Independencia.*

1. El Comité actuará con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias con arreglo a los artículos 70 y 71.

2. Sin perjuicio de las solicitudes de la Comisión contempladas en el artículo 70, apartados 1 y 2, el Comité no solicitará ni admitirá instrucciones de nadie en el desempeño de sus funciones o el ejercicio de sus competencias.

Artículo 70. *Funciones del Comité.*

1. El Comité garantizará la aplicación coherente del presente Reglamento. A tal efecto, el Comité, a iniciativa propia o, en su caso, a instancia de la Comisión, en particular:

a) supervisará y garantizará la correcta aplicación del presente Reglamento en los casos contemplados en los artículos 64 y 65, sin perjuicio de las funciones de las autoridades de control nacionales;

b) asesorará a la Comisión sobre toda cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación del presente Reglamento;

c) asesorará a la Comisión sobre el formato y los procedimientos para intercambiar información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes;

d) emitirá directrices, recomendaciones y buenas prácticas relativas a los procedimientos para la supresión de vínculos, copias o réplicas de los datos personales procedentes de servicios de comunicación a disposición pública a que se refiere el artículo 17, apartado 2;

e) examinará, a iniciativa propia, a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del presente Reglamento, y emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del presente Reglamento;

f) emitirá directrices, recomendaciones y buenas prácticas de conformidad con la letra e) del presente apartado a fin de especificar más los criterios y requisitos de las decisiones basadas en perfiles en virtud del artículo 22, apartado 2;

g) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de constatar las violaciones de la seguridad de los datos y determinar la dilación indebida a tenor del artículo 33, apartados 1 y 2, y con respecto a las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales;

h) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con respecto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas a tenor del artículo 34, apartado 1;

i) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con el fin de especificar en mayor medida los criterios y requisitos para las transferencias de datos personales basadas en normas corporativas vinculantes a las que se hayan adherido los responsables del tratamiento y en normas corporativas vinculantes a las que se hayan adherido los encargados del tratamiento y en requisitos adicionales necesarios para garantizar la protección de los datos personales de los interesados a que se refiere el artículo 47;

j) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de especificar en mayor medida los criterios y requisitos de las transferencias de datos personales sobre la base del artículo 49, apartado 1;

k) formulará directrices para las autoridades de control, relativas a la aplicación de las medidas a que se refiere el artículo 58, apartados 1, 2 y 3, y la fijación de multas administrativas de conformidad con el artículo 83;

l) examinará la aplicación práctica de las directrices, recomendaciones y buenas prácticas;

m) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de establecer procedimientos comunes de información procedente de personas físicas sobre infracciones del presente Reglamento en virtud del artículo 54, apartado 2;

n) alentará la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos de conformidad con los artículos 40 y 42;

o) aprobará los criterios de certificación en virtud del artículo 42, apartado 5, y llevará un registro público de los mecanismos de certificación y sellos y marcas de protección de datos en virtud del artículo 42, apartado 8, y de los responsables o los encargados del tratamiento certificados establecidos en terceros países en virtud del artículo 42, apartado 7;

p) aprobará los requisitos contemplados en el artículo 43, apartado 3, con miras a la acreditación de los organismos de certificación a los que se refiere el artículo 43;

q) facilitará a la Comisión un dictamen sobre los requisitos de certificación contemplados en el artículo 43, apartado 8;

r) facilitará a la Comisión un dictamen sobre los iconos a que se refiere el artículo 12, apartado 7;

s) facilitará a la Comisión un dictamen para evaluar la adecuación del nivel de protección en un tercer país u organización internacional, en particular para evaluar si un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o una organización internacional, ya no garantizan un nivel de protección adecuado. A tal fin, la Comisión facilitará al Comité toda la documentación necesaria, incluida la correspondencia con el gobierno del tercer país, que se refiera a dicho tercer país, territorio o específico o a dicha organización internacional;

t) emitirá dictámenes sobre los proyectos de decisión de las autoridades de control en virtud del mecanismo de coherencia mencionado en el artículo 64, apartado 1, sobre los asuntos presentados en virtud del artículo 64, apartado 2, y sobre las decisiones vinculantes en virtud del artículo 65, incluidos los casos mencionados en el artículo 66;

u) promoverá la cooperación y los intercambios bilaterales y multilaterales efectivos de información y de buenas prácticas entre las autoridades de control;

v) promoverá programas de formación comunes y facilitará intercambios de personal entre las autoridades de control y, cuando proceda, con las autoridades de control de terceros países o con organizaciones internacionales;

w) promoverá el intercambio de conocimientos y documentación sobre legislación y prácticas en materia de protección de datos con las autoridades de control encargadas de la protección de datos a escala mundial;

x) emitirá dictámenes sobre los códigos de conducta elaborados a escala de la Unión de conformidad con el artículo 40, apartado 9, y

y) llevará un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

2. Cuando la Comisión solicite asesoramiento del Comité podrá señalar un plazo teniendo en cuenta la urgencia del asunto.

3. El Comité transmitirá sus dictámenes, directrices, recomendaciones y buenas prácticas a la Comisión y al Comité contemplado en el artículo 93, y los hará públicos.

4. Cuando proceda, el Comité consultará a las partes interesadas y les dará la oportunidad de presentar sus comentarios en un plazo razonable. Sin perjuicio de lo dispuesto en el artículo 76, el Comité publicará los resultados del procedimiento de consulta.

Artículo 71. *Informes.*

1. El Comité elaborará un informe anual en materia de protección de las personas físicas en lo que respecta al tratamiento en la Unión y, si procede, en terceros países y organizaciones internacionales. El informe se hará público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión.

2. El informe anual incluirá un examen de la aplicación práctica de las directrices, recomendaciones y buenas prácticas indicadas en el artículo 70, apartado 1, letra l), así como de las decisiones vinculantes indicadas en el artículo 65.

Artículo 72. *Procedimiento.*

1. El Comité tomará sus decisiones por mayoría simple de sus miembros, salvo que el presente Reglamento disponga otra cosa.
2. El Comité adoptará su reglamento interno por mayoría de dos tercios de sus miembros y organizará sus disposiciones de funcionamiento.

Artículo 73. *Presidencia.*

1. El Comité elegirá por mayoría simple de entre sus miembros un presidente y dos vicepresidentes.
2. El mandato del presidente y de los vicepresidentes será de cinco años de duración y podrá renovarse una vez.

Artículo 74. *Funciones del presidente.*

1. El presidente desempeñará las siguientes funciones:

a) convocar las reuniones del Comité y preparar su orden del día;
b) notificar las decisiones adoptadas por el Comité con arreglo al artículo 65 a la autoridad de control principal y a las autoridades de control interesadas;
c) garantizar el ejercicio puntual de las funciones del Comité, en particular en relación con el mecanismo de coherencia a que se refiere el artículo 63.

2. El Comité determinará la distribución de funciones entre el presidente y los vicepresidentes en su reglamento interno.

Artículo 75. *Secretaría.*

1. El Comité contará con una secretaría, de la que se hará cargo el Supervisor Europeo de Protección de Datos.
2. La secretaría ejercerá sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité.
3. El personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento dependerá de un superior jerárquico distinto del personal que desempeñe las funciones conferidas al Supervisor Europeo de Protección de Datos.
4. El Comité, en consulta con el Supervisor Europeo de Protección de Datos, elaborará y publicará, si procede, un memorando de entendimiento para la puesta en práctica del presente artículo, que determinará los términos de su cooperación y que será aplicable al personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento.
5. La secretaría prestará apoyo analítico, administrativo y logístico al Comité.
6. La secretaría será responsable, en particular, de:

a) los asuntos corrientes del Comité;
b) la comunicación entre los miembros del Comité, su presidente y la Comisión;
c) la comunicación con otras instituciones y con el público;
d) la utilización de medios electrónicos para la comunicación interna y externa;
e) la traducción de la información pertinente;
f) la preparación y el seguimiento de las reuniones del Comité;
g) la preparación, redacción y publicación de dictámenes, decisiones relativas a solución de diferencias entre autoridades de control y otros textos adoptados por el Comité.

Artículo 76. *Confidencialidad.*

1. Los debates del Comité serán confidenciales cuando el mismo lo considere necesario, tal como establezca su reglamento interno.

2. El acceso a los documentos presentados a los miembros del Comité, los expertos y los representantes de terceras partes se regirá por el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo [21].

[21] Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

CAPÍTULO VIII

Recursos, responsabilidad y sanciones

Artículo 77. *Derecho a presentar una reclamación ante una autoridad de control.*

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.

2. La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 78.

Artículo 78. *Derecho a la tutela judicial efectiva contra una autoridad de control.*

1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente en virtud de los artículos 55 y 56 no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77.

3. Las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control.

4. Cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o una decisión del Comité en el marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión.

Artículo 79. *Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento.*

1. Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

2. Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

Artículo 80. *Representación de los interesados.*

1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el

ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.

2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento.

Artículo 81. *Suspensión de los procedimientos.*

1. Cuando un tribunal competente de un Estado miembro tenga información de la pendencia ante un tribunal de otro Estado miembro de un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado, se pondrá en contacto con dicho tribunal de otro Estado miembro para confirmar la existencia de dicho procedimiento.

2. Cuando un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado esté pendiente ante un tribunal de otro Estado miembro, cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento.

3. Cuando dicho procedimiento esté pendiente en primera instancia, cualquier tribunal distinto de aquel ante el que se ejercitó la acción en primer lugar podrá también, a instancia de una de las partes, inhibirse en caso de que el primer tribunal sea competente para su conocimiento y su acumulación sea conforme a Derecho.

Artículo 82. *Derecho a indemnización y responsabilidad.*

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2.

6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2.

Artículo 83. *Condiciones generales para la imposición de multas administrativas.*

1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones del organismo de supervisión a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 84. *Sanciones.*

1. Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable.

CAPÍTULO IX

Disposiciones relativas a situaciones específicas de tratamiento

Artículo 85. *Tratamiento y libertad de expresión y de información.*

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.

3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

Artículo 86. *Tratamiento y acceso del público a documentos oficiales.*

Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento.

Artículo 87. *Tratamiento del número nacional de identificación.*

Los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento.

Artículo 88. *Tratamiento en el ámbito laboral.*

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleadores o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 89. *Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.*

1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre y cuando sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuando esas excepciones sean necesarias para alcanzar esos fines.

3. Cuando se traten datos personales con fines de archivo en interés público, el Derecho de le Unión o de los Estados miembros podrá prever excepciones a los derechos contemplados en los artículos 15, 16, 18, 19, 20 y 21, sujetas a las condiciones y garantías citadas en el apartado 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

4. En caso de que el tratamiento a que hacen referencia los apartados 2 y 3 sirva también al mismo tiempo a otro fin, las excepciones solo serán aplicables al tratamiento para los fines mencionados en dichos apartados.

Artículo 90. *Obligaciones de secreto.*

1. Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control establecidos en el artículo 58, apartado 1, letras e) y f), en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes, cuando sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto. Esas normas solo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado o con ocasión de una actividad cubierta por la citada obligación de secreto.

2. Cada Estado miembro notificará a la Comisión las normas adoptadas de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 91. *Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.*

1. Cuando en un Estado miembro iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del presente Reglamento, un conjunto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento, tales normas podrán seguir aplicándose, siempre que sean conformes con el presente Reglamento.

2. Las iglesias y las asociaciones religiosas que apliquen normas generales de conformidad con el apartado 1 del presente artículo estarán sujetas al control de una autoridad de control independiente, que podrá ser específica, siempre que cumpla las condiciones establecidas en el capítulo VI del presente Reglamento.

CAPÍTULO X

Actos delegados y actos de ejecución

Artículo 92. *Ejercicio de la delegación.*

1. Los poderes para adoptar actos delegados otorgados a la Comisión estarán sujetos a las condiciones establecidas en el presente artículo.

2. La delegación de poderes indicada en el artículo 12, apartado 8, y en el artículo 43, apartado 8, se otorgarán a la Comisión por tiempo indefinido a partir del 24 de mayo de 2016.

3. La delegación de poderes mencionada en el artículo 12, apartado 8, y el artículo 43, apartado 8, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto al día siguiente de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Los actos delegados adoptados en virtud del artículo 12, apartado 8, y el artículo 43, apartado 8, entrarán en vigor únicamente si, en un plazo de tres meses desde su notificación

al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. El plazo se ampliará en tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 93. *Procedimiento de comité.*

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. Cuando se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

3. Cuando se haga referencia al presente apartado, se aplicará el artículo 8 del Reglamento (UE) n.º 182/2011, en relación con su artículo 5.

CAPÍTULO XI

Disposiciones finales

Artículo 94. *Derogación de la Directiva 95/46/CE.*

1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018.

2. Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.

Artículo 95. *Relación con la Directiva 2002/58/CE.*

El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE.

Artículo 96. *Relación con acuerdos celebrados anteriormente.*

Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados por los Estados miembros antes del 24 de mayo de 2016 y que cumplan lo dispuesto en el Derecho de la Unión aplicable antes de dicha fecha, seguirán en vigor hasta que sean modificados, sustituidos o revocados.

Artículo 97. *Informes de la Comisión.*

1. A más tardar el 25 de mayo de 2020 y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.

2. En el marco de las evaluaciones y revisiones a que se refiere el apartado 1, la Comisión examinará en particular la aplicación y el funcionamiento de:

a) el capítulo V sobre la transferencia de datos personales a países terceros u organizaciones internacionales, particularmente respecto de las decisiones adoptadas en virtud del artículo 45, apartado 3, del presente Reglamento, y de las adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE;

b) el capítulo VII sobre cooperación y coherencia.

3. A los efectos del apartado 1, la Comisión podrá solicitar información a los Estados miembros y a las autoridades de control.

4. Al llevar a cabo las evaluaciones y revisiones indicadas en los apartados 1 y 2, la Comisión tendrá en cuenta las posiciones y conclusiones del Parlamento Europeo, el Consejo y los demás órganos o fuentes pertinentes.

5. La Comisión presentará, en caso necesario, las propuestas oportunas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de las tecnologías de la información y a la vista de los progresos en la sociedad de la información.

Artículo 98. *Revisión de otros actos jurídicos de la Unión en materia de protección de datos.*

La Comisión presentará, si procede, propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos.

Artículo 99. *Entrada en vigor y aplicación.*

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.
2. Será aplicable a partir del 25 de mayo de 2018.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

§ 10

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 106, de 4 de mayo de 2022
Última modificación: 6 de noviembre de 2024
Referencia: BOE-A-2022-7191

I

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) tenía por objeto determinar la política de seguridad en la utilización de medios electrónicos de las entidades de su ámbito de aplicación, estando constituido por los principios básicos y requisitos mínimos que han venido garantizando adecuadamente la seguridad de la información tratada y los servicios prestados por dichas entidades.

El ENS, cuyo ámbito de aplicación comprendía todas las entidades de las administraciones públicas, perseguía fundamentar la confianza en que los sistemas de información prestan sus servicios adecuadamente y custodian la información sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a personas no autorizadas, estableciendo medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de forma que se facilite a los ciudadanos y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos.

Desde 2010 se han producido notables cambios en España y en la Unión Europea, incluidos la progresiva transformación digital de nuestra sociedad, el nuevo escenario de la ciberseguridad y el avance de las tecnologías de aplicación. Asimismo, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, advirtiéndose un notable incremento de los ciberataques, tanto en volumen y frecuencia como en sofisticación, con agentes y actores con mayores capacidades técnicas y operativas; amenazas que se producen en un contexto de alta dependencia de las tecnologías de la información y de las comunicaciones en nuestra sociedad y de gran interconexión de los sistemas de información. Todo ello afecta significativamente a un número cada vez mayor de entidades públicas y privadas, a sus cadenas de suministro, a los ciudadanos y, por ende, a la ciberseguridad nacional, lo que compromete el normal desenvolvimiento social y económico del país y el ejercicio de los derechos y libertades de los ciudadanos, como reconocen tanto la Estrategia de Ciberseguridad Nacional de 2013 como, particularmente, la Estrategia Nacional de Ciberseguridad 2019.

El Real Decreto 3/2010, de 8 de enero, establecía que el ENS debía desarrollarse y perfeccionarse manteniéndose actualizado de forma permanente conforme al progreso de los servicios de la administración electrónica, de la evolución de la tecnología, de los nuevos

estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo.

En el plano normativo, acompasado a dichos cambios y en ocasiones como origen de los mismos, desde 2010 se han modificado tanto el marco europeo (con cuatro Reglamentos y una Directiva) como el español, referido a la seguridad nacional, regulación del procedimiento administrativo y el régimen jurídico del sector público, de protección de datos personales y de la seguridad de las redes y sistemas de información, y se ha evolucionado el marco estratégico de la ciberseguridad.

Así, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera a la ciberseguridad como un ámbito de especial interés de la Seguridad Nacional tal como señala su artículo 10, y que, por ello, requiere una atención específica por resultar básica para preservar los derechos y libertades y el bienestar de los ciudadanos y para garantizar el suministro de los servicios y recursos esenciales. De acuerdo con las previsiones de su artículo 4.3 se aprobó el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017, y posteriormente, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, identificando en ambas al ciberespacio como un espacio común global, que la Estrategia 2021 describe como espacio de conexión caracterizado por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad, añadiendo que en los espacios comunes globales resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13 incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

En desarrollo de las dos leyes anteriores, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, concreta en diferentes preceptos la obligación del cumplimiento de las medidas de seguridad previstas en el ENS, como los referidos al intercambio electrónico de datos en entornos cerrados de comunicación, los sistemas de clave concertada y otros sistemas de identificación de las personas interesadas, el archivo electrónico único o los portales de internet, entre otros.

Coincidente en el tiempo con la aprobación de las tres leyes mencionadas, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, actualizó el ENS a la luz de la experiencia y conocimiento en su aplicación, de la situación de la ciberseguridad del momento, y de la evolución del marco legal, para adecuarse a lo previsto en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (conocido como «Reglamento eIDAS»).

Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ordenó en su disposición adicional primera que dichas medidas de seguridad se implanten en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679, del

Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). De otra parte, la disposición adicional primera también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales. Por último, y en el mismo sentido, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ha establecido en su artículo 37 la obligación de aplicar las medidas del ENS a los tratamientos de datos personales por parte de las autoridades públicas competentes.

Por otra parte, con relación a la seguridad de redes y sistemas de información, desde la entrada en vigor del Real Decreto 3/2010, de 8 de enero, se han aprobado en la Unión Europea dos Reglamentos y una Directiva que han fijado el marco de actuación en los ordenamientos nacionales.

Así, en primer lugar, el Reglamento (UE) N.º 526/2013 del Parlamento Europeo y del Consejo de 21 de mayo de 2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) N.º 460/2004. En segundo lugar, el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»).

En tercer lugar, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS (*Security of Network and Information Systems)*», que ha sido objeto de transposición en España por medio del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, señalando la necesidad de tener en cuenta el ENS en el momento de elaborar las disposiciones reglamentarias, instrucciones y guías, y adoptar las medidas aplicables a entidades del ámbito de aplicación de este. Este Real Decreto-ley 12/2018, de 7 de septiembre, ha sido desarrollado por el Real Decreto 43/2021, de 26 de enero, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad. Así, el Real Decreto 43/2021, de 26 de enero, establece que las medidas para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero.

Tal como estableció la Estrategia de Seguridad Nacional de 2017, España precisa garantizar un uso seguro y responsable de las redes y sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable. En este sentido, el Consejo de Seguridad Nacional aprobó el 12 de abril de 2019 la Estrategia Nacional de Ciberseguridad 2019, publicada por Orden PCI/487/2019, de 26 de abril, con el propósito de fijar las directrices generales en el ámbito de la ciberseguridad de manera que se alcanzasen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

La Estrategia Nacional de Ciberseguridad 2019, contiene un objetivo general y cinco objetivos específicos, y, para alcanzarlos, se proponen siete líneas de acción con un total de 65 medidas. El primero de estos objetivos es la seguridad y resiliencia de las redes y sistemas de información y comunicaciones del sector público y de los servicios esenciales y se desarrolla a través de dos líneas de acción y veinticuatro medidas específicas entre las que figura la de asegurar la plena implantación del Esquema Nacional de Seguridad. Para desarrollar esta Estrategia, el Consejo de Ministros ha aprobado el 29 de marzo de 2022 el

Plan Nacional de Ciberseguridad, que prevé cerca de 150 iniciativas, entre actuaciones y proyectos, para los próximos tres años.

Asimismo, la Estrategia Nacional de Ciberseguridad 2019 señala entre sus objetivos la consolidación de un marco nacional coherente e integrado que garantice la protección de la información y de los datos personales tratados por los sistemas y redes del sector público y de los servicios, sean o no esenciales, recogiendo que su cumplimiento requiere la implantación de medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, mediante el desarrollo de nuevas soluciones, y el refuerzo de la coordinación y la adaptación del ordenamiento jurídico.

II

La evolución de las amenazas, los nuevos vectores de ataque, el desarrollo de modernos mecanismos de respuesta y la necesidad de mantener la conformidad y el alineamiento con las regulaciones europeas y nacionales de aplicación, exigen adaptar las medidas de seguridad a esta nueva realidad. Fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa.

Por ello, en un mundo hiperconectado como el actual, implementar la seguridad en el ciberespacio se ha convertido en una prioridad estratégica. Sin embargo, el riesgo en el ciberespacio es demasiado grande para que el sector público o las empresas lo aborden por sí solos, pues ambos comparten el interés y la responsabilidad de enfrentar juntos ese reto. A medida que aumenta el papel de la tecnología en la sociedad, la ciberseguridad se convierte en un desafío cada vez mayor.

De hecho, el pasado 9 de marzo, el Parlamento Europeo ha aprobado por amplísima mayoría una Resolución sobre injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación. Tal como señala dicha Resolución en sus considerandos, las injerencias extranjeras constituyen un patrón de conducta que amenaza o afecta negativamente a valores, procedimientos democráticos, procesos políticos, la seguridad de Estados y ciudadanos y la capacidad de hacer frente a situaciones excepcionales. Las tácticas de injerencia extranjera, que se combinan a menudo para tener un mayor efecto, adoptan, entre otras formas, los ciberataques, la asunción del control de infraestructuras críticas, la desinformación, supresión de información, manipulación de plataformas de redes sociales y de sus algoritmos, operaciones de pirateo y filtración, amenazas y acoso para acceder a información sobre los votantes e interferir en la legitimidad del proceso electoral, personalidades e identidades falsas, ejercicio de presiones sobre ciudadanos extranjeros que viven en la Unión, instrumentalización de migrantes y espionaje.

Al tiempo que el escenario descrito ha venido consolidándose, se ha ido extendiendo la implantación del ENS, resultando de ello una mayor experiencia acumulada sobre su aplicación, a la vez que un mejor conocimiento de la situación gracias a las sucesivas ediciones del Informe Nacional del Estado de la Seguridad (INES), del cuerpo de guías de seguridad CCN-STIC y de los servicios y herramientas proporcionados por la capacidad de respuesta a incidentes de seguridad de la información, el CCN-CERT, del Centro Criptológico Nacional (CCN).

En definitiva, por todas las razones anteriormente expuestas es necesario actualizar el ENS para cumplir tres grandes objetivos.

En primer lugar, alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital. Se trata de reflejar con claridad el ámbito de aplicación del ENS en beneficio de la ciberseguridad y de los derechos de los ciudadanos, así como de actualizar las referencias al marco legal vigente y de revisar la formulación de ciertas cuestiones a la luz de éste, conforme a la Estrategia Nacional de Ciberseguridad 2019 y el Plan Nacional de Ciberseguridad, de forma que se logre simplificar, precisar o armonizar los mandatos del ENS, eliminar aspectos que puedan considerarse excesivos, o añadir aquellos otros que se identifican como necesarios.

En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de «perfil de cumplimiento específico» que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

En tercer lugar, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Por último, la aprobación de este real decreto se incardina también en la ejecución del Plan de Digitalización de las Administraciones Públicas 2021-2025, uno de los instrumentos principales para el cumplimiento del Plan de Recuperación, Transformación y Resiliencia y su Componente 11 denominado «Modernización de las Administraciones Públicas», así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025. Dicho Plan de Digitalización contempla expresamente, entre sus reformas, la actualización del ENS con el fin de hacer evolucionar la política de seguridad de todas las entidades del sector público español, tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información. Dicha reforma se ve complementada con la constitución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos que servirá de referencia para las demás administraciones públicas y contribuirá a mejorar el cumplimiento del ENS de las entidades en su alcance de servicio. Esta previsión ha sido respaldada por el Acuerdo de Consejo de Ministros de 25 de mayo de 2021 sobre actuaciones urgentes en materia de ciberseguridad que mandata la tramitación y aprobación de un real decreto que sustituya al Real Decreto 3/2010, de 8 de enero, como medida de refuerzo del marco normativo.

III

El real decreto se estructura en cuarenta y un artículos distribuidos en siete capítulos, tres disposiciones adicionales, una disposición transitoria, una disposición derogatoria, tres disposiciones finales y cuatro anexos.

El capítulo I comprende las disposiciones generales que regulan el objeto de la norma, su ámbito de aplicación, la referencia a los sistemas de información que traten datos personales y las definiciones aplicables. El ámbito de aplicación es el previsto en el artículo 2 de la Ley 40/2015, de 1 de octubre, al que se añaden los sistemas que tratan información clasificada, sin perjuicio de la normativa que resulte de aplicación, pudiendo resultar necesario complementar las medidas de seguridad de este real decreto con otras específicas para tales sistemas, derivadas de los compromisos internacionales contraídos por España o su pertenencia a organismos o foros internacionales en la materia. Asimismo los requisitos del ENS serán de aplicación a los sistemas de información de las entidades del sector privado, cuando de acuerdo con la normativa aplicable y en virtud de una relación contractual presten servicios a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas. Como se ha señalado anteriormente, considerando que la transformación digital ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y que el sector privado se encuentra igualmente inmerso en la transformación digital de sus procesos de negocio, ambos tipos de sistemas de información se encuentran expuestos al mismo tipo de amenazas y riesgos. Por ello, los operadores del sector privado que prestan servicios a las entidades del sector público, por razón de la alta imbricación de unos y otras, han de garantizar el mismo nivel de seguridad que se aplica a los sistemas y a la información en el ámbito del sector público, todo ello de conformidad, además, con los especiales requerimientos establecidos tanto en la Ley Orgánica 3/2018, de 5 de diciembre, como en la Ley Orgánica 7/2021, de 26 de mayo. Por otra parte, cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo

establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

El capítulo II, que comprende los artículos 5 a 11, regula los principios básicos que deben regir el ENS y que enumera en su artículo 5: seguridad integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua y reevaluación periódica; y diferenciación de responsabilidades.

El capítulo III se refiere a la Política de Seguridad y los requisitos mínimos para permitir una protección adecuada de la información y los servicios. En los artículos 12 a 27 se definen tales requisitos: organización e implantación del proceso de seguridad; gestión de riesgos, consistente en un proceso de identificación, análisis, evaluación y tratamiento de los mismos; gestión de personal; profesionalidad; autorización y control de los accesos; protección de las instalaciones; adquisición de productos de seguridad y contratación de servicios de seguridad; mínimo privilegio; integridad y actualización del sistema; protección de la información almacenada y en tránsito; prevención ante otros sistemas de información interconectados; registro de la actividad y detección de código dañino; incidentes de seguridad; continuidad de la actividad; y mejora continua del proceso de seguridad. Seguidamente, el artículo 28 indica que para el cumplimiento de tales requisitos mínimos deberán adoptarse las medidas recogidas en el anexo II, conforme a una serie de consideraciones al efecto. No obstante, tales medidas de seguridad podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que la protección que aportan es, al menos, equivalente, y satisfacen los principios básicos y requisitos mínimos indicados previamente. En el artículo 29 se hace un llamamiento a la utilización de infraestructuras y servicios comunes de las administraciones públicas en aras de lograr una mayor eficiencia y retroalimentación de las sinergias de cada colectivo. Por último, el artículo 30 establece la posibilidad de implementar perfiles de cumplimiento específicos, así como esquemas de acreditación de entidades de implementación de configuraciones seguras.

El capítulo IV versa sobre la auditoría de la seguridad, el informe del estado de la seguridad y la respuesta a incidentes de seguridad. La auditoría de la seguridad se desarrolla íntegramente en el artículo 31, detallando las características del procedimiento de auditoría, así como de los correspondientes informes. Por su parte, el artículo 32, relativo al informe del estado de la seguridad, destaca el papel de la Comisión Sectorial de Administración Electrónica en este ámbito, así como del CCN y los órganos colegiados competentes en el ámbito de la administración digital en la Administración General del Estado.

La prevención, detección y respuesta a incidentes de seguridad se regula en los artículos 33 y 34, separando, por un lado, los aspectos relativos a la capacidad de respuesta y, por otro, los relativo a la prestación de los servicios de respuesta a incidentes de seguridad, tanto a las entidades del Sector Público como a las organizaciones del sector privado que les presten servicios.

En el capítulo V, artículos 35 a 38, se definen las normas de conformidad, que se concretan en cuatro: Administración Digital, ciclo de vida de servicios y sistemas, mecanismos de control y procedimientos de determinación de la conformidad con el ENS.

Por su parte, el capítulo VI, compuesto por su único artículo, el 39, establece la obligación de actualización permanente, de acuerdo con el marco jurídico vigente en cada momento, la evolución de la tecnología y los estándares en materia de seguridad y sistemas, así como de las ya mencionadas nuevas amenazas y vectores de ataque.

Concluye el articulado de la parte dispositiva con el capítulo VII, que desarrolla el procedimiento de categorización de los sistemas de información, definiendo en el artículo 40 las categorías de seguridad y en el artículo 41 las facultades al respecto.

En cuanto a las tres disposiciones adicionales, la primera regula los programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público que desarrollarán el CCN y el Instituto Nacional de Administración Pública.

La segunda disposición adicional regula las instrucciones técnicas de seguridad, de obligado cumplimiento y las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC).

Por último, la tercera disposición adicional establece el cumplimiento del llamado principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH, por sus siglas en inglés, *Do No Significant Harm)* y las condiciones del etiquetado climático y digital.

La disposición transitoria única fija un plazo de veinticuatro meses para que los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, alcancen su plena adecuación al ENS.

La disposición derogatoria suprime el Real Decreto 3/2010, de 8 de enero, así como cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Por último, la norma cuenta con tres disposiciones finales. La primera de ellas enumera los títulos competenciales; la segunda disposición final habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la su aplicación y desarrollo, sin perjuicio de las competencias de las comunidades autónomas para el desarrollo y ejecución de la legislación básica del Estado, y la disposición final tercera ordena la entrada en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

El real decreto se complementa con cuatro anexos: el anexo I regula las categorías de seguridad de los sistemas de información, detallando la secuencia de actuaciones para determinar la categoría de seguridad de un sistema; el anexo II detalla las medidas de seguridad; el anexo III se ocupa del objeto, niveles e interpretación de la Auditoría de la seguridad y, por último, el anexo IV incluye el glosario de términos y definiciones.

Con relación, en particular, al anexo II, este detalla las medidas de seguridad estructuradas en tres grupos: el marco organizativo, constituido por el conjunto de medidas relacionadas con la organización global de la seguridad; el marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin; y las medidas de protección, que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas. Como se ha dicho, la modificación del marco táctico y operativo en el que se desenvuelven las ciberamenazas y sus correlativas salvaguardas ha obligado a actualizar el elenco de medidas de seguridad del anexo II, con objeto de añadir, eliminar o modificar controles y sub-controles, al tiempo que se incluye un nuevo sistema de referencias más moderno y adecuado, sobre la base de la existencia de un requisito general y de unos posibles refuerzos, alineados con el nivel de seguridad perseguido. Todo ello se efectúa con el objetivo de afianzar de manera proporcionada la seguridad de los sistemas de información concernidos, y facilitar su implantación y auditoría.

IV

El real decreto, cuya aprobación está incluida en el Plan Anual Normativo de la Administración General del Estado para el año 2022, se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia).

Así, la norma es acorde con los principios de necesidad y eficacia en tanto que persigue un interés general al concretar la regulación del ENS desarrollando en este aspecto la Ley 40/2015, de 1 de octubre y otros aspectos concretos de la normativa nacional y de la Unión Europea mencionada en este preámbulo. La norma es también acorde con el principio de proporcionalidad, al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento, estableciéndose un marco normativo estable, integrado y claro. Durante el procedimiento de elaboración de la norma y aún en el contexto de la aplicación de las previsiones del artículo 27 de la Ley 50/1997, de 27 de noviembre, del Gobierno, por tratarse de una tramitación de urgencia acordada por el Consejo de Ministros, se han formalizado los trámites de audiencia e información pública, conforme a lo previsto en el artículo 133 de la Ley 39/2015, de 1 de octubre, y el artículo 26 de la Ley 50/1997, de 27 de noviembre, en cumplimiento del principio de transparencia,

quedando además justificados en el preámbulo los objetivos que persigue este real decreto. El proyecto se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y ha sido informado por la Comisión Nacional de los Mercados y la Competencia A.A.I. y la Agencia Española de Protección de Datos A.A.I.

Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación en materia de cargas administrativas, respecto de la normativa que desarrolla.

El real decreto se aprueba en ejercicio de las competencias previstas en los artículos 149.1.18.ª, 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, sobre las telecomunicaciones y sobre la seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital, con la aprobación previa de la Ministra de Hacienda y Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 3 de mayo de 2022,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Este real decreto tiene por objeto regular el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

3. Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Artículo 2. *Ámbito de aplicación.*

1. El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

2. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales.

3. Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto

contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

4. Cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

Artículo 3. *Sistemas de información que traten datos personales.*

1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

Artículo 4. *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el Glosario de términos incluido en el anexo IV.

CAPÍTULO II

Principios básicos

Artículo 5. *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.
c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Vigilancia continua.
f) Reevaluación periódica.
g) Diferenciación de responsabilidades.

Artículo 6. *La seguridad como un proceso integral.*

1. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

Artículo 7. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

2. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Artículo 8. *Prevención, detección, respuesta y conservación.*

1. La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

2. Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

3. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

4. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Artículo 9. *Existencia de líneas de defensa.*

1. El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.

b) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Artículo 10. *Vigilancia continua y reevaluación periódica.*

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

2. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Artículo 11. *Diferenciación de responsabilidades.*

1. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

3. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

CAPÍTULO III

Política de seguridad y requisitos mínimos de seguridad

Artículo 12. *Política de seguridad y requisitos mínimos de seguridad.*

1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

a) Los objetivos o misión de la organización.

b) El marco regulatorio en el que se desarrollarán las actividades.

c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

f) Los riesgos que se derivan del tratamiento de los datos personales.

2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.

No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.

3. En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Los organismos públicos y entidades pertenecientes al sector público institucional estatal podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento con el que mantenga la relación de vinculación, dependencia o adscripción, o bien quedar comprendidos en el ámbito subjetivo de la política de seguridad de este. También podrán contar con su propia política de seguridad, aprobada por el órgano competente, coherente con la del Departamento del que dependan o al que estén adscritos, los centros directivos de la propia Administración General del Estado que gestionen servicios bajo la declaración de servicios compartidos.

4. La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital dispondrá de su propia política de seguridad, que será aprobada por la persona titular de la misma.

5. Los municipios podrán disponer de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales.

6. La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de la actividad y detección de código dañino.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
ñ) Mejora continua del proceso de seguridad.

7. Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos.

Artículo 13. *Organización e implantación del proceso de seguridad.*

1. La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.
2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

a) El responsable de la información determinará los requisitos de la información tratada
b) El responsable del servicio determinará los requisitos de los servicios prestados.
c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

3. El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.
4. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.
5. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

Artículo 14. *Análisis y gestión de los riesgos.*

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de servicios realizará su propia gestión de riesgos.
2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.
3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Artículo 15. *Gestión de personal.*

1. El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.
2. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente.

Artículo 16. *Profesionalidad.*

1. La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.
2. Las entidades del ámbito de aplicación de este real decreto exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
3. Las organizaciones determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

Artículo 17. *Autorización y control de los accesos.*

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Artículo 18. *Protección de las instalaciones.*

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Artículo 19. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

1. En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los

sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

2. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
b) Otras certificaciones de seguridad adicionales que se requieran normativamente.
c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

3. Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

Artículo 20. *Mínimo privilegio.*

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Artículo 21. *Integridad y actualización del sistema.*

1. La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.
2. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

Artículo 22. *Protección de información almacenada y en tránsito.*

1. En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.
2. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.
3. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que

correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Artículo 23. *Prevención ante otros sistemas de información interconectados.*

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Artículo 24. *Registro de actividad y detección de código dañino.*

1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

3. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Artículo 25. *Incidentes de seguridad.*

1. La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 26. *Continuidad de la actividad.*

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Artículo 27. *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Artículo 28. *Cumplimiento de los requisitos mínimos.*

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:

a) Los activos que constituyen los sistemas de información concernidos.
b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Las medidas a las que se refiere el apartado 1 tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados. La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

3. Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, del riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III. Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implantadas y las medidas del anexo II que compensan. El conjunto será objeto de la aprobación formal por parte del responsable de la seguridad. Una Guía CCN-STIC de las previstas en la disposición adicional segunda guiará en la selección de dichas medidas, así como su registro e inclusión en la Declaración de Aplicabilidad.

Artículo 29. *Infraestructuras y servicios comunes.*

La utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto. Los supuestos concretos de utilización de estas infraestructuras y servicios serán determinados por cada administración pública.

Artículo 30. *Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras.*

1. En virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

2. De forma análoga a lo dispuesto en el apartado anterior, para posibilitar la adecuada implantación y configuración de soluciones o plataformas suministradas por terceros, que vayan a ser usadas por las entidades comprendidas en el ámbito de aplicación de este real decreto, se podrán implementar esquemas de acreditación de entidades y validación de personas, que garanticen la seguridad de dichas soluciones o plataformas y la conformidad con lo dispuesto en este real decreto.

3. El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan y los antedichos esquemas de acreditación y validación, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda.

4. Las correspondientes instrucciones técnicas de seguridad o, en su caso, las guías de Seguridad CCN-STIC, precisarán las condiciones a las que deberán sujetarse las implementaciones en modo local de productos, sistemas o servicios originariamente

prestados en la nube o en forma remota, así como las condiciones específicas para su evaluación y auditoría.

CAPÍTULO IV

Seguridad de los sistemas: auditoría, informe e incidentes de seguridad

Artículo 31. *Auditoría de la seguridad.*

1. Los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

El plazo de dos años señalado en los párrafos anteriores podrá extenderse durante tres meses cuando concurran impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

2. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

3. En la realización de las auditorías de la seguridad se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de actividades.

4. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas, todo ello de conformidad con la citada Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

5. Los informes de auditoría serán presentados al responsable del sistema y al responsable de la seguridad. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

6. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, el responsable del sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

7. Los informes de auditoría podrán ser requeridos por los responsables de cada organización, con competencias sobre seguridad de las tecnologías de la información, y por el CCN.

Artículo 32. *Informe del estado de la seguridad.*

1. La Comisión Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere este real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las entidades titulares de los sistemas de información comprendidos en el ámbito de aplicación del artículo 2, que se plasmará en el informe correspondiente.

2. El CCN articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en la Comisión Sectorial de Administración Electrónica y en los órganos colegiados competentes en el ámbito de la Administración General del Estado.

3. Los resultados del informe serán utilizados por las autoridades competentes que impulsarán las medidas oportunas que faciliten la mejora continua del estado de la seguridad utilizando en su caso, cuadros de mando e indicadores que contribuyan a la toma de decisiones mediante el uso de las herramientas que el CCN provea para tal efecto.

Artículo 33. *Capacidad de respuesta a incidentes de seguridad.*

1. El CCN articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (por su acrónimo en inglés de *Computer Emergency Response Team),* que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

2. Sin perjuicio de lo establecido en el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre, las entidades del sector público notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, de acuerdo con la correspondiente Instrucción Técnica de Seguridad.

3. Cuando un operador esencial que haya sido designado como operador crítico sufra un incidente, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de su Oficina de Coordinación de Ciberseguridad, según lo previsto en el artículo 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, éste pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas, lo pondrá de inmediato en conocimiento de su CSIRT de referencia, quien informará a la capacidad de respuesta e incidentes de seguridad de referencia para el ámbito de la Defensa nacional, denominada ESPDEF-CERT, del Mando Conjunto del Ciberespacio (MCCE) a través de los canales establecidos. En estos casos, el ESPDEF-CERT del Mando Conjunto del Ciberespacio deberá ser oportunamente informado de la evolución de la gestión del incidente y podrá colaborar en la supervisión con la autoridad competente.

5. De conformidad con lo dispuesto en el Real Decreto-ley 12/2018, de 7 de septiembre, el CCN ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (denominados por su acrónimo en inglés *Computer Security Incident Response Team,* en adelante, CSIRT) en materia de seguridad de las redes y sistemas de información del sector público.

6. Tras un incidente de seguridad, el CCN-CERT determinará técnicamente el riesgo de reconexión del sistema o sistemas afectados, indicando los procedimientos a seguir y las salvaguardas a implementar con objeto de reducir el impacto para, en la medida de lo posible, evitar que vuelvan a darse las circunstancias que lo propiciaron.

Tras un incidente de seguridad, la Secretaría General de Administración Digital, sin perjuicio de la normativa que regula la continuidad de los sistemas de información implicados en la seguridad pública o la normativa que regule la continuidad de los sistemas de información militares implicados en la Defensa Nacional que requieran la participación del ESPDEF-CERT del Mando Conjunto del Ciberespacio, autorizará la reconexión a los medios y servicios comunes comprendidos bajo su ámbito de responsabilidad, incluidos los compartidos o transversales, si un informe de superficie de exposición del CCN-CERT hubiere determinado que el riesgo es asumible.

En caso de que se trate de un incidente de seguridad que afecte a un medio o servicio común bajo ámbito de responsabilidad de la Intervención General de la Administración del Estado, esta participará en el proceso de autorización de la reconexión a que se refiere el párrafo anterior.

7. Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán al INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) dependiente del Ministerio de Asuntos Económicos y Transformación Digital, los incidentes que les afecten a través de su equipo de respuesta a incidentes de seguridad informática, quien, sin perjuicio de sus competencias y de lo previsto en los artículos 9, 10 y 11 del Real Decreto 43/2021, de

26 de enero, en relación con la Plataforma de Notificación y Seguimiento de Ciberincidentes, lo pondrá inmediatamente en conocimiento del CCN-CERT.

Artículo 34. *Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público.*

1. De acuerdo con lo previsto en el artículo 33, el CCN-CERT prestará los siguientes servicios:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las entidades del ámbito de aplicación de este real decreto.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información afectados.

Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar informes, registros de auditoría y configuraciones de los sistemas afectados y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la normativa de protección de datos que resulte de aplicación, así como de la posible confidencialidad de datos de carácter institucional u organizativo.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las entidades del sector público. Con esta finalidad, las series de documentos CCN-STIC (CCN-Seguridad de las Tecnologías de Información y la Comunicación), elaboradas por el CCN, ofrecerán normas, instrucciones, guías, recomendaciones y mejores prácticas para aplicar el ENS y para garantizar la seguridad de los sistemas de información del ámbito de aplicación de este real decreto.

c) Formación destinada al personal del sector público especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos y de lograr la sensibilización y mejora de sus capacidades para la prevención, detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las entidades del sector público puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquel, será coordinador a nivel público estatal.

CAPÍTULO V

Normas de conformidad

Artículo 35. *Administración digital.*

1. La seguridad de los sistemas de información que sustentan la administración digital se regirá por lo establecido en este real decreto.

2. El CCN es el órgano competente para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.

Artículo 36. *Ciclo de vida de servicios y sistemas.*

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Artículo 37. *Mecanismos de control.*

Cada entidad titular de los sistemas de información comprendidos en el ámbito de aplicación de este real decreto y, en su caso, sus organismos, órganos, departamentos o

unidades, establecerán sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento del ENS.

Artículo 38. *Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad.*

1. Los sistemas de información comprendidos en el ámbito del artículo 2 serán objeto de un proceso para determinar su conformidad con el ENS. A tal efecto, los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir asimismo para los fines de la certificación, mientras que los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, sin perjuicio de que se puedan someter igualmente a una auditoria de certificación.

Tanto el procedimiento de autoevaluación como la auditoría de certificación se realizarán según lo dispuesto en el artículo 31 y el anexo III y en los términos que se determinen en la correspondiente Instrucción Técnica de Seguridad, que concretará asimismo los requisitos exigibles a las entidades certificadoras.

2. Los sujetos responsables de los sistemas de información a que se refiere el apartado anterior darán publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la mencionada Instrucción Técnica de Seguridad.

CAPÍTULO VI

Actualización del Esquema Nacional de Seguridad

Artículo 39. *Actualización permanente.*

El ENS se mantendrá actualizado de manera permanente, desarrollándose y perfeccionándose a lo largo del tiempo, en paralelo al avance de los servicios prestados por las entidades del sector público, la evolución tecnológica, la aparición o consolidación de nuevos estándares internacionales sobre seguridad y auditoría y los riesgos a los que estén expuestos los sistemas de información concernidos.

CAPÍTULO VII

Categorización de los sistemas de información

Artículo 40. *Categorías de seguridad.*

1. La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

2. La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I.

Artículo 41. *Facultades.*

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 40, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados.

2. Con base en las valoraciones señaladas en el apartado anterior, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad.

Disposición adicional primera. *Formación.*

El CCN y el Instituto Nacional de Administración Pública desarrollarán programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público, para asegurar un adecuado despliegue de la información y las capacidades jurídicas, organizativas y técnicas relacionadas con la ciberseguridad de los sistemas de información públicos, y para garantizar el conocimiento permanente del ENS entre dichas entidades.

Disposición adicional segunda. *Desarrollo del Esquema Nacional de Seguridad.*

En desarrollo de lo dispuesto en este real decreto, la persona titular del Ministerio para la Transformación Digital y de la Función Pública, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de la persona titular de la Secretaría de Estado de Función Pública.

Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas por la Unión Europea aplicables. Para su redacción y mantenimiento se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración digital.

Para el mejor cumplimiento de lo establecido en este real decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

Disposición adicional tercera. *Respeto del principio de «no causar un perjuicio significativo» al medioambiente.*

En cumplimiento con lo dispuesto en el Plan de Recuperación, Transformación y Resiliencia (PRTR) y en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, todas las actuaciones que se lleven a cabo en el marco del PRTR en cumplimiento del presente real decreto deben respetar el principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH por sus siglas en inglés, *Do No Significant Harm)* y las condiciones del etiquetado climático y digital.

Disposición transitoria única. *Adecuación de sistemas.*

1. Los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, incluidos aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS, circunstancia que se manifestará con la exhibición del correspondiente distintivo de conformidad, atendiendo lo dispuesto en el artículo 38.

2. Durante los antedichos veinticuatro meses, los sistemas de información preexistentes a la entrada en vigor de este real decreto que dispusieren de los correspondientes Distintivos de Conformidad, derivados de Declaraciones o Certificaciones de conformidad con el ENS, podrán mantener su vigencia procediendo a su renovación de conformidad y en los términos señalados por el Real Decreto 3/2010, de 8 de enero, del que trajeron causa.

3. Los nuevos sistemas de información aplicarán lo establecido en este real decreto desde su concepción.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como cuantas disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Títulos competenciales.*

Este real decreto se dicta en virtud de lo establecido en los artículos 149.1.18.ª, 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, las telecomunicaciones y la seguridad pública, respectivamente.

Disposición final segunda. *Desarrollo normativo.*

Se habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en este real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

Este real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Categorías de seguridad de los sistemas de información

1. Fundamentos para la determinación de la categoría de seguridad de un sistema de información

La determinación de la categoría de seguridad de un sistema de información se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Garantizar la conformidad con el ordenamiento jurídico.

Anualmente, o siempre que se produzcan modificaciones significativas en los citados criterios de determinación, deberá re-evaluarse la categoría de seguridad de los sistemas de información concernidos.

2. Dimensiones de la seguridad

A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas:

a) Confidencialidad [C].
b) Integridad [I].
c) Trazabilidad [T].
d) Autenticidad [A].
e) Disponibilidad [D].

3. Determinación del nivel de seguridad requerido en una dimensión de seguridad

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles de seguridad: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1.º La reducción de forma apreciable de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2.º Causar un daño menor en los activos de la organización.
3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4.º Causar un perjuicio menor a algún individuo, que pese a resultar molesto, pueda ser fácilmente reparable.
5.º Otros de naturaleza análoga.

b) Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio grave:

1.º La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2.º Causar un daño significativo en los activos de la organización.
3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.
5.º Otros de naturaleza análoga.

c) Nivel ALTO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio muy grave:

1.º La anulación efectiva de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias.
2.º Causar un daño muy grave, e incluso irreparable, de los activos de la organización.
3.º El incumplimiento grave de alguna ley o regulación.
4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5.º Otros de naturaleza análoga.

Cuando un sistema de información trate diferentes informaciones y preste diferentes servicios, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4. Determinación de la categoría de seguridad de un sistema de información

1. Se definen tres categorías de seguridad: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.
b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad superior.
c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

2. La determinación de la categoría de seguridad de un sistema de información sobre la base de lo indicado en el apartado anterior, no implicará que se altere, por este hecho, el nivel de seguridad de las dimensiones de seguridad que no han influido en la determinación de la categoría de seguridad del mismo.

5. Secuencia de actuaciones para determinar la categoría de seguridad de un sistema

1. Identificación del nivel de seguridad correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3 anterior.

2. Determinación de la categoría de seguridad del sistema, según lo establecido en el apartado 4 anterior.

Las guías CCN-STIC, del CCN, precisarán los criterios necesarios para una adecuada categorización de seguridad de los sistemas de información.

ANEXO II

Medidas de Seguridad

1. Disposiciones generales

1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

a) Las dimensiones de seguridad relevantes en el sistema a proteger.
b) La categoría de seguridad del sistema de información a proteger.

2. Las medidas de seguridad se dividen en tres grupos:

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

2. Selección de medidas de seguridad

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

a) Identificación de los tipos de activos presentes.
b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
c) Determinación del nivel de seguridad correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
d) Determinación de la categoría de seguridad del sistema, según lo establecido en el anexo I.
e) Selección de las medidas de seguridad, junto con los refuerzos apropiados, de entre las contenidas en este anexo, de acuerdo con las dimensiones y sus niveles de seguridad y para determinadas medidas de seguridad, de acuerdo con la categoría de seguridad del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan subsistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad con los refuerzos correspondientes, y siempre que puedan delimitarse la información y los servicios afectados.

3. Las guías CCN-STIC, del CCN, podrán establecer perfiles de cumplimiento específicos, según el artículo 30 de este real decreto, para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables o los criterios para su determinación.

4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad con sus refuerzos, es la que se indica en la tabla siguiente:

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org	**Marco organizativo**				
org.1	Política de seguridad	Categoría	aplica	aplica	aplica
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
op	**Marco operacional**				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	Explotación				
op.exp.1	Inventario de activos	Categoría	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Categoría	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	aplica
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	+ R1
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	+ R1
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	+ R1 + R2
op.cont	Continuidad del servicio				
op.cont.1	Análisis de impacto	D	n.a.	aplica	aplica
op.cont.2	Plan de continuidad	D	n.a.	n.a.	aplica
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	aplica
op.cont.4	Medios alternativos	D	n.a.	n.a.	aplica
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
mp	Medidas de protección				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica
mp.if.6	Protección frente a inundaciones	D	n.a.	aplica	aplica
mp.if.7	Registro de entrada y salida de equipamiento	Categoría	aplica	aplica	aplica
mp.per	Gestión del personal				
mp.per.1	Caracterización del puesto de trabajo	Categoría	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Categoría	aplica	+ R1	+ R1
mp.per.3	Concienciación	Categoría	aplica	aplica	aplica
mp.per.4	Formación	Categoría	aplica	aplica	aplica
mp.eq	Protección de los equipos				
mp.eq.1	Puesto de trabajo despejado	Categoría	aplica	+ R1	+ R1
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.eq.4	Otros dispositivos conectados a la red	C	aplica	+ R1	+ R1
mp.com	Protección de las comunicaciones				
mp.com.1	Perímetro seguro	Categoría	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separación de flujos de información en la red	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
mp.si	Protección de los soportes de información				
mp.si.1	Marcado de soportes	C	n.a.	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1 + R2
mp.si.3	Custodia	Categoría	aplica	aplica	aplica
mp.si.4	Transporte	Categoría	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	+ R1	+ R1

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
mp.sw	Protección de las aplicaciones informáticas				
mp.sw.1	Desarrollo de aplicaciones	Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Categoría	aplica	+ R1	+ R1
mp.info	Protección de la información				
mp.info.1	Datos personales	Categoría	aplica	aplica	aplica
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.3	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4
mp.info.4	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.5	Limpieza de documentos	C	aplica	aplica	aplica
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2
mp.s	Protección de los servicios				
mp.s.1	Protección del correo electrónico	Categoría	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Categoría	aplica	aplica	+ R1
mp.s.4	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

5. En las tablas del presente anexo se han empleado las siguientes convenciones:

a) La tercera columna indica si la medida se exige atendiendo al nivel de seguridad de una o más dimensiones de seguridad, o atendiendo a la categoría de seguridad del sistema. Cuando se exija por nivel de seguridad de las dimensiones, se indican cuales afectan utilizando sus iniciales.

b) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad, en algún nivel de seguridad determinado, se utiliza la voz «aplica».

c) «n.a.» significa «no aplica» a efectos de cumplimiento normativo, por lo que no es exigible, sin perjuicio de que su implantación en el sistema pudiera ser beneficioso técnicamente.

d) Para indicar una mayor exigencia se emplean los refuerzos de seguridad (R) que se suman (+) a los requisitos base de la medida pero que no siempre son incrementales entre sí.

e) Para señalar que se puede elegir entre aplicar un refuerzo u otro, se indicará entre corchetes y separados por «o» [Rn o Rn+1].

f) Se han empleado los colores verde, amarillo y rojo con el siguiente código: verde para indicar que una medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar qué medidas y refuerzos empiezan a aplicar en categoría MEDIA o superior; y el rojo para indicar qué medidas o refuerzos son solo de aplicación en categoría ALTA o requieren un esfuerzo en seguridad superior al de categoría MEDIA.

6. A continuación, se describen individualmente cada una de las medidas organizadas de la siguiente forma:

a) Primero, una tabla resumen con las exigencias de seguridad de la medida en función de la categoría de seguridad del sistema y de las dimensiones de seguridad afectadas.

b) A continuación, una descripción con el cuerpo de la medida que desglosa los requisitos de base.

c) Posteriormente, podrán aparecer una serie de refuerzos adicionales que complementan a los requisitos de base, no en todos los casos requeridos o exigidos, y que podrían aplicarse en determinados perfiles de cumplimiento específicos.

d) Además, se indica el conjunto de requisitos y refuerzos exigidos en función de los niveles de seguridad o de la categoría de seguridad del sistema, según corresponda. En los casos en los que se pueda elegir entre aplicar un refuerzo u otro, además de indicarlo entre corchetes [Rm o Rn], se incluirá un diagrama de flujo explicativo.

e) Por último, algunos refuerzos son de carácter opcional, no siendo requeridos en todos los sistemas de información. Se aplicarán como medidas adicionales cuando el análisis de riesgos así lo recomiende.

3. Marco organizativo [ORG]

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este real decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

– [org.1.1] Los objetivos o misión de la organización.
– [org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.
– [org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
– [org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.
– [org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Aplicación de la medida.

– Categoría BÁSICA: org.1.
– Categoría MEDIA: org.1.
– Categoría ALTA: org.1.

3.2 Normativa de seguridad [org.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se dispondrá de una serie de documentos que describan:

– [org.2.1] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.
– [org.2.2] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Refuerzo R1-Documentos específicos.

[org.2.r1.1] Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación.

Aplicación de la medida.

– Categoría BÁSICA: org.2.
– Categoría MEDIA: org.2.
– Categoría ALTA: org.2.

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	aplica	aplica

Requisitos.

Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

– [org.3.1] Cómo llevar a cabo las tareas habituales.
– [org.3.2] Quién debe hacer cada tarea.
– [org.3.3] Cómo identificar y reportar comportamientos anómalos.
– [org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:

a) Su control de acceso.
b) Su almacenamiento.
c) La realización de copias.
d) El etiquetado de soportes.
e) Su transmisión telemática.
f) Cualquier otra actividad relacionada con dicha información.

Refuerzo R1-Validación de procedimientos.

[org.3.r1.1] Se requerirá la validación de los procedimientos de seguridad por la autoridad correspondiente.

Aplicación de la medida.

– Categoría BÁSICA: org.3.
– Categoría MEDIA: org.3.
– Categoría ALTA: org.3.

3.4 Proceso de autorización [org.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos:

– [org.4.1] Utilización de instalaciones, habituales y alternativas.
– [org.4.2] Entrada de equipos en producción, en particular, equipos que involucren criptografía.
– [org.4.3] Entrada de aplicaciones en producción.
– [org.4.4] Establecimiento de enlaces de comunicaciones con otros sistemas.
– [org.4.5] Utilización de medios de comunicación, habituales y alternativos.
– [org.4.6] Utilización de soportes de información.
– [org.4.7] Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.
– [org.4.8] Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.

Aplicación de la medida.

– Categoría BÁSICA: org.4.
– Categoría MEDIA: org.4.
– Categoría ALTA: org.4.

4. Marco operacional [op]

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R2

Requisitos.

Se realizará un análisis de riesgos informal, realizado en lenguaje natural. Es decir, una exposición textual que:

– [op.pl.1.1] Identifique los activos más valiosos del sistema. (Ver op.exp.1).
– [op.pl.1.2] Identifique las amenazas más probables.
– [op.pl.1.3] Identifique las salvaguardas que protegen de dichas amenazas.
– [op.pl.1.4] Identifique los principales riesgos residuales.

Refuerzo R1-Análisis de riesgos semiformal.

Se deberá realizar un análisis de riesgos semiformal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que:

– [op.pl.1.r1.1] Valore cualitativamente los activos más valiosos del sistema.
– [op.pl.1.r1.2] Cuantifique las amenazas más probables.
– [op.pl.1.r1.3] Valore las salvaguardas que protegen de dichas amenazas.
– [op.pl.1.r1.4] Valore el riesgo residual.

Refuerzo R2-Análisis de riesgos formal.

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente, que:

– [op.pl.1.r2.1] Valore cualitativamente los activos más valiosos del sistema.
– [op.pl.1.r2.2] Cuantifique las amenazas posibles.
– [op.pl.1.r2.3] Valore y priorice las salvaguardas adecuadas.
– [op.pl.1.r2.4] Valore y asuma formalmente el riesgo residual.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.1.
– Categoría MEDIA: op.pl.1 + R1.
– Categoría ALTA: op.pl.1 + R2.

4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

– [op.pl.2.1] Documentación de las instalaciones, incluyendo áreas y puntos de acceso.
– [op.pl.2.2] Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración).
– [op.pl.2.3] Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

– [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Refuerzo R1-Sistema de gestión.

[op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Refuerzo R2-Sistema de gestión de la seguridad con mejora continua.

[op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

Refuerzo R3-Validación de datos.

[op.pl.2.r3.1] Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.2.
– Categoría MEDIA: op.pl.2 + R1.
– Categoría ALTA: op.pl.2 + R1 + R2 + R3.

4.1.3 Adquisición de nuevos componentes [op.pl.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

– [op.pl.3.1] Atenderá a las conclusiones del análisis de riesgos ([op.pl.1]).
– [op.pl.3.2] Será acorde a la arquitectura de seguridad escogida ([op.pl.2]).
– [op.pl.3.3] Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.3.
– Categoría MEDIA: op.pl.3.
– Categoría ALTA: op.pl.3.

4.1.4 Dimensionamiento / gestión de la capacidad [op.pl.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos:

– [op.pl.4.1] Necesidades de procesamiento.
– [op.pl.4.2] Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
– [op.pl.4.3] Necesidades de comunicación.
– [op.pl.4.4] Necesidades de personal: cantidad y cualificación profesional.
– [op.pl.4.5] Necesidades de instalaciones y medios auxiliares.

Refuerzo R1 –Mejora continua de la gestión de la capacidad.

– [op.pl.4.r1.1] Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.
– [op.pl.4.r1.2] Se emplearán herramientas y recursos para la monitorización de la capacidad.

Aplicación de la medida (por disponibilidad):

– Nivel BAJO: op.pl.4.
– Nivel MEDIO: op.pl.4 + R1.
– Nivel ALTO: op.pl.4 + R1.

4.1.5 Componentes certificados [op.pl.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [op.pl.5.1]. Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.
En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.
Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.
– [op.pl.5.2] Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

Refuerzo R1-Protección de emisiones electromagnéticas.

[op.pl.5.r1.1] La información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor.

Refuerzo R2 - Lista de componentes software.

[op.pl.5.r2.1] Cada producto y servicio incluirá en su descripción una lista de componentes software, acorde a lo especificado en [mp.sw.1.r5].

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.pl.5.
– Categoría ALTA: op.pl.5.

4.2 Control de acceso [op.acc].

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.
Los mecanismos de control de acceso deberán equilibrar la facilidad de uso y la protección de la información y los servicios, primando una u otra característica atendiendo a la categoría de seguridad del sistema.
Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se

acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

4.2.1 Identificación [op.acc.1].

dimensiones	T A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

– [op.acc.1.1] Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

– [op.acc.1.2] Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

– [op.acc.1.3] Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

– [op.acc.1.4] Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario.

c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará «periodo de retención».

– [op.acc.1.5] En los supuestos de comunicaciones electrónicas, las partes intervinientes se identificarán atendiendo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y sus normas de desarrollo o ejecución que resulten de aplicación:

a) Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

b) Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

c) Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento (UE) n.º 910/2014).

Refuerzo R1-Identificación avanzada.

– [op.acc.1.r1.1] La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

– [op.acc.1.r1.2] Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad.
– [op.acc.1.r1.3] Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

Aplicación de la medida (por trazabilidad y autenticidad).

– Nivel BAJO: op.acc.1.
– Nivel MEDIO: op.acc.1 +R1.
– Nivel ALTO: op.acc.1+ R1.

4.2.2 Requisitos de acceso [op.acc.2].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	+ R1

Requisitos.

– [op.acc.2.1] Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.
– [op.acc.2.2] Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.
– [op.acc.2.3] Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.

Refuerzo R1-Privilegios de acceso.

– [op.acc.2.r1.1] Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.
– [op.acc.2.r1.2] Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.).

Refuerzo R2-Control de acceso a dispositivos.

– [op.acc.2.r2.1] Se dispondrá de soluciones que permitan establecer controles de acceso a los dispositivos en función de la política de seguridad de la organización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.2.
– Nivel MEDIO: op.acc.2.
– Nivel ALTO: op.acc.2+ R1.

4.2.3 Segregación de funciones y tareas [op.acc.3].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita o no autorizada.

– [op.acc.3.1] Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.
– [op.acc.3.2] Siempre que sea posible, las personas que autorizan y controlan el uso serán distintas.

Refuerzo R1-Segregación rigurosa.

– [op.acc.3.r1.1] Siempre que sea posible, la misma persona no aunará funciones de configuración y mantenimiento del sistema.
– [op.acc.3.r1.2] La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función.

Refuerzo R2-Privilegios de auditoría.

– [op.acc.3.r2.1] Existirán cuentas con privilegios de auditoría estrictamente controladas y personalizadas.

Refuerzo R3-Acceso a la información de seguridad.

– [op.acc.3.r3.1] El acceso a la información de seguridad del sistema estará permitido únicamente a los administradores de seguridad/sistema autorizados, utilizando los mecanismos de acceso imprescindibles (consola, interfaz web, acceso remoto, etc.).

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: op.acc.3.
– Nivel ALTO: op.acc.3 + R1.

4.2.4 Proceso de gestión de derechos de acceso [op.acc.4].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:

– [op.acc.4.1] Todo acceso estará prohibido, salvo autorización expresa.
– [op.acc.4.2] Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.
– [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.
– [op.acc.4.4] Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.
– [op.acc.4.5] Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

Nivel BAJO: op.acc.4.
Nivel MEDIO: op.acc.4.
Nivel ALTO: op.acc.4.

4.2.5 Mecanismo de autenticación (usuarios externos) [op.acc.5].

Referente a usuarios que no son usuarios de la organización.
Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A

nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5

Requisitos.

– [op.acc.5.1] Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.

– [op.acc.5.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.

– [op.acc.5.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.

– [op.acc.5.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.

– [op.acc.5.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.

– [op.acc.5.6] Las credenciales serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

– [op.acc.5.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

– [op.acc.5.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.

– [op.acc.5.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.5.r1.1] Se empleará una contraseña como mecanismo de autenticación.

– [op.acc.5.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + OTP.

– [op.acc.5.r2.1] Se requerirá una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario.

Refuerzo R3-Certificados.

– [op.acc.5.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.

– [op.acc.5.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

– [op.acc.5.r3.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.5.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.

– [op.acc.5.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

– [op.acc.5.r4.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

Refuerzo R5-Registro.

– [op.acc.5.r5.1] Se registrarán los accesos con éxito y los fallidos.
– [op.acc.5.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.5.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.5.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.5 + [R1 o R2 o R3 o R4].
– Nivel MEDIO: op.acc.5 + [R2 o R3 o R4] + R5.
– Nivel ALTO: op.acc.5 + [R2 o R3 o R4] + R5.

4.2.6 Mecanismo de autenticación (usuarios de la organización) [op.acc.6].

Esta medida se refiere a personal del organismo, propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en el sistema.

Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación, en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9

Requisitos.

– [op.acc.6.1] Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten.
– [op.acc.6.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.
– [op.acc.6.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
– [op.acc.6.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.
– [op.acc.6.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.
– [op.acc.6.6] Las credenciales serán inhabilitadas cuando el usuario que autentican termina su relación con el sistema.
– [op.acc.6.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

– [op.acc.6.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
– [op.acc.6.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.6.r1.1] Se empleará una contraseña como mecanismo de autenticación cuando el acceso se realiza desde zonas controladas y sin atravesar zonas no controladas (véase refuerzo R8).
– [op.acc.6.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + otro factor de autenticación.

– [op.acc.6.r2.1] Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».

Refuerzo R3-Certificados.

– [op.acc.6.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.
– [op.acc.6.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.6.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.
– [op.acc.6.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R5-Registro.

– [op.acc.6.r5.1] Se registrarán los accesos con éxito y los fallidos.
– [op.acc.6.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.6.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.6.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Refuerzo R8-Doble factor para acceso desde o a través de zonas no controladas.

Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet.

– [op.acc.6.r8.1] Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación: R2, R3 o R4.

Refuerzo R9-Acceso remoto (todos los niveles).

– [op.acc.6.r9.1] Será de aplicación la ITS de Interconexión de sistemas de información.
– [op.acc.6.r9.2] El acceso remoto deberá considerar los siguientes aspectos:

a) Ser autorizado por la autoridad correspondiente.
b) El tráfico deberá ser cifrado.

c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario.
d) Deberán recogerse registros de auditoría de este tipo de conexiones.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.6 + [R1 o R2 o R3 o R4] + R8 + R9.
– Nivel MEDIO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R8 + R9.
– Nivel ALTO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9.

4.3 Explotación [op.exp].

4.3.1 Inventario de activos [op.exp.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[op.exp.1.1] Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo.

Refuerzo R1-Inventario de etiquetado.

– [op.exp.1.r1.1] El etiquetado del equipamiento y del cableado formará parte del inventario.

Refuerzo R2-Identificación periódica de activos.

– [op.exp.1.r2.1] Se dispondrá de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular, los servidores y los dispositivos de red y de comunicaciones.

Refuerzo R3-Identificación de activos críticos.

– [op.exp.1.r3.1] Se dispondrá de herramientas que permitan categorizar los activos críticos por contexto de la organización y riesgos de seguridad.

Refuerzo R4-Lista de componentes software.

– [op.exp.1.r4.1] Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5].

Aplicación de la medida.

– Categoría BÁSICA: op.exp.1.
– Categoría MEDIA: op.exp.1.
– Categoría ALTA: op.exp.1.

4.3.2 Configuración de seguridad [op.exp.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se configurarán los equipos previamente a su entrada en operación, de forma que:

– [op.exp.2.1] Se retiren cuentas y contraseñas estándar.
– [op.exp.2.2] Se aplicará la regla de «mínima funcionalidad», es decir:

a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos.
b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.

– [op.exp.2.3] Se aplicará la regla de «seguridad por defecto», es decir:

a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes.
c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

– [op.exp.2.4] Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro. La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.2.
– Categoría MEDIA: op.exp.2.
– Categoría ALTA: op.exp.2.

4.3.3 Gestión de la configuración de seguridad [op.exp.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

Se gestionará de forma continua la configuración de los componentes del sistema, de forma que:

– [op.exp.3.1] Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).
– [op.exp.3.2] Se mantenga en todo momento la regla de "mínimo privilegio" ([op.exp.2]).
– [op.exp.3.3] El sistema se adapte a las nuevas necesidades, previamente autorizadas. (Ver [op.acc.4]).
– [op.exp.3.4] El sistema reaccione a vulnerabilidades notificadas. (Ver [op.exp.4]).
– [op.exp.3.5] El sistema reaccione a incidentes. (Ver [op.exp.7]).
– [op.exp.3.6] La configuración de seguridad solamente podrá editarse por personal debidamente autorizado.

Refuerzo R1-Mantenimiento regular de la configuración.

– [op.exp.3.r1.1] Existirán configuraciones hardware/software, autorizadas y mantenidas regularmente, para los servidores, elementos de red y estaciones de trabajo.
– [op.exp.3.r1.2] Se verificará periódicamente la configuración hardware/software del sistema para asegurar que no se han introducido ni instalado elementos no autorizados.
– [op.exp.3.r1.3] Se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

Refuerzo R2-Responsabilidad de la configuración.
– [op.exp.3.r2.1] La configuración de seguridad del sistema operativo y aplicaciones, tanto de estaciones y servidores como de la electrónica de red del sistema, será responsabilidad de un número muy limitado de administradores del sistema.

Refuerzo R3-Copias de seguridad.

– [op.exp.3.r3.1] Se realizarán copias de seguridad de la configuración del sistema de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

Refuerzo R4-Aplicación de la configuración.

– [op.exp.3.r4.1] La configuración de seguridad del sistema operativo y de las aplicaciones se mantendrá actualizada a través de una aplicación o procedimiento manual que permita la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas.

Refuerzo R5-Control del estado de seguridad de la Configuración.

– [op.exp.3.r5.1] Se dispondrá de herramientas que permitan conocer de forma periódica el estado de seguridad de la configuración de los dispositivos de red y, en el caso de que resulte deficiente, permitir su corrección.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.3.
– Categoría MEDIA: op.exp.3 + R1.
– Categoría ALTA: op.exp.3 + R1 + R2 + R3.

4.3.4 Mantenimiento y actualizaciones de seguridad [op.exp.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

– [op.exp.4.1] Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.
– [op.exp.4.2] Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.
– [op.exp.4.3] El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Refuerzo R1-Pruebas en preproducción.

[op.exp.4.r1.1] Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

Refuerzo R2-Prevención de fallos.

[op.exp.4.r2.1] Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad se preverá un mecanismo para revertirlos en caso de aparición de efectos adversos.

Refuerzo R3-Actualizaciones y pruebas periódicas.

[op.exp.4.r3.1] Se deberá comprobar de forma periódica la integridad del firmware utilizado en los dispositivos hardware del sistema (infraestructura de red, BIOS, etc.). La periodicidad de estas comprobaciones seguirá las recomendaciones de la Guía CCN-STIC que sea de aplicación.

Refuerzo R4 - Monitorización continua.

[op.exp.4.r4.1] Se desplegará a nivel de sistema una estrategia de monitorización continua de amenazas y vulnerabilidades. Esta estrategia detallará:

1. Los indicadores críticos de seguridad a emplear.

2. La política de aplicación de parches de seguridad de los componentes software relacionados en las listas de [op.exp.1.r4], [op.ext.3.r3] y [mp.sw.1.r5]).
3. Los criterios de revisión regular y excepcional de las amenazas sobre el sistema.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.4.
– Categoría MEDIA: op.exp.4 + R1.
– Categoría ALTA: op.exp.4 + R1 + R2.

4.3.5 Gestión de cambios [op.exp.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

Se mantendrá un control continuo de los cambios realizados en el sistema, de forma que:

– [op.exp.5.1] Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio se registrarán asignando un número de referencia que permita su seguimiento, de forma equivalente al registro de los incidentes.
– [op.exp.5.2] La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.
– [op.exp.5.3] Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.
– [op.exp.5.4] Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados, explícitamente, de forma previa a su implantación, por el Responsable de la Seguridad.
– [op.exp.5.5] Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

Refuerzo R1-Prevención de fallos.

– [op.exp.5.r1.1] Antes de la aplicación de los cambios, se deberá tener en cuenta la posibilidad de revertirlos en caso de la aparición de efectos adversos.
– [op.exp.5.r1.2] Todos los fallos en el software y hardware deberán ser comunicados al responsable designado en la organización de la seguridad.
– [op.exp.5.r1.3] Todos los cambios en el sistema deberán documentarse, incluyendo una valoración del impacto que dicho cambio supone en la seguridad del sistema.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.exp.5.
– Categoría ALTA: op.exp.5+ R1.

4.3.6 Protección frente a código dañino [op.exp.6].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+R1+R2+R3+R4

Requisitos.

– [op.exp.6.1] Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante.
– [op.exp.6.2] Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales.
– [op.exp.6.3] Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.
– [op.exp.6.4] Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas.
– [op.exp.6.5] El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Refuerzo R1-Escaneo periódico.

– [op.exp.6.r1.1] Todo el sistema se escaneará regularmente para detectar código dañino.

Refuerzo R2-Revisión preventiva del sistema.

– [op.exp.6.r2.1] Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

Refuerzo R3 - Lista blanca.

– [op.exp.6.r3.1] Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas.

Refuerzo R4-Capacidad de respuesta en caso de incidente.

– [op.exp.6.r4.1] Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - *Endpoint Detection and Response*).

Refuerzo R5-Configuración de la herramienta de detección de código dañino.

– [op.exp.6.r5.1] El software de detección de código dañino permitirá realizar configuraciones avanzadas y revisar el sistema en el arranque y cada vez que se conecte un dispositivo extraíble.
– [op.exp.6.r5.2] El software de detección de código dañino instalado en servidores y elementos perimetrales deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.6.
– Categoría MEDIA: op.exp.6+ R1 + R2.
– Categoría ALTA: op.exp.6+ R1 + R2 + R3 + R4.

4.3.7 Gestión de incidentes [op.exp.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2+ R3

Requisitos.

– [op.exp.7.1] Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
– [op.exp.7.2] La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5

de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.

Refuerzo R1-Notificación.

– [op.exp.7.r1.1] Se dispondrá de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

Refuerzo R2 –Detección y Respuesta.

El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema ([op.exp.7.1]) deberá incluir:

– [op.exp.7.r2.1] Implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
– [op.exp.7.r2.2] Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
– [op.exp.7.r2.3] Informar del incidente a los responsables de la información y servicios afectados y de las actuaciones llevadas a cabo para su resolución.
– [op.exp.7.r2.4] Medidas para:

a) Prevenir que se repita el incidente.
b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

Refuerzo R3-Reconfiguración dinámica.

La reconfiguración dinámica del sistema persigue detener, desviar o limitar ataques, acotando los daños.
– [op.exp.7.r3.1] La reconfiguración dinámica incluye, por ejemplo, cambios en las reglas de los enrutadores (*routers*), listas de control de acceso, parámetros del sistema de detección / prevención de intrusiones y reglas en los cortafuegos y puertas de enlace, aislamiento de elementos críticos y aislamiento de las copias de seguridad.
– [op.exp.7.r3.2] El organismo adaptará los procedimientos de reconfiguración dinámica reaccionando a los anuncios recibidos del CCN-CERT relativos a ciberamenazas sofisticadas y campañas de ataques.

Refuerzo R4-Prevención y Respuesta Automática.

– [op.exp.7.r4.1] Se dispondrá de herramientas que automaticen el proceso de prevención y respuesta mediante la detección e identificación de anomalías, la segmentación dinámica de la red para reducir la superficie de ataque, el aislamiento de dispositivos críticos, etc.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.7.
– Categoría MEDIA: op.exp.7+ R1 + R2.
– Categoría ALTA: op.exp.7+ R1 + R2 + R3.

4.3.8 Registro de la actividad [op.exp.8].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5

Requisitos.

Se registrarán las actividades en el sistema, de forma que:

– [op.exp.8.1] Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma.
– [op.exp.8.2] Se activarán los registros de actividad en los servidores.

Refuerzo R1-Revisión de los registros.

– [op.exp.8.r1.1] Se revisarán informalmente, de forma periódica, los registros de actividad, buscando patrones anormales.

Refuerzo R2-Sincronización del reloj del sistema.

– [op.exp.8.r2.1] El sistema deberá disponer de una referencia de tiempo (*timestamp*) para facilitar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.

Refuerzo R3-Retención de registros.

– [op.exp.8.r3.1] En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.

Refuerzo R4-Control de acceso.

– [op.exp.8.r4.1] Los registros de actividad y, en su caso, las copias de seguridad de los mismos, solamente podrán ser accedidos o eliminarse por personal debidamente autorizado.

Refuerzo R5-Revisión automática y correlación de eventos.

– [op.exp.8.r5.1] El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales.
– [op.exp.8.r5.2] Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

Aplicación de la medida (por trazabilidad).

– Nivel BAJO: op.exp.8.
– Nivel MEDIO: op.exp.8 + R1 + R2 + R3 + R4.
– Nivel ALTO: op.exp.8 + R1 + R2 + R3 + R4 + R5.

4.3.9 Registro de la gestión de incidentes [op.exp.9].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

– [op.exp.9.1] Se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.
– [op.exp.9.2] Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.
– [op.exp.9.3] Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.9.
– Categoría MEDIA: op.exp.9.
– Categoría ALTA: op.exp.9.

4.3.10 Protección de claves criptográficas [op.exp.10].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

– [op.exp.10.1] Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.
– [op.exp.10.2] Los medios de generación estarán aislados de los medios de explotación.
– [op.exp.10.3] Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Refuerzo R1-Algoritmos autorizados.

– [op.exp.10.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Protección avanzada de claves criptográficas.

– [op.exp.10.r2.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.10.
– Categoría MEDIA: op.exp.10 + R1.
– Categoría ALTA: op.exp.10 + R1.

4.4 Recursos externos [op.ext].

Cuando la organización utilice recursos externos (servicios, productos, instalaciones o personal), mantendrá la plena responsabilidad de los riesgos para la información tratada o los servicios prestados, debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.

4.4.1 Contratación y acuerdos de nivel de servicio [op.ext.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [op.ext.1.1] Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.1.
– Categoría ALTA: op.ext.1.

4.4.2 Gestión diaria [op.ext.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

Se establecerá lo siguiente:

– [op.ext.2.1] Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
– [op.ext.2.2] El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres (ver [op.exp.7]).

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.2.
– Categoría ALTA: op.ext.2.

4.4.3 Protección de la cadena de suministro [op.ext.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	n.a.	aplica

Requisitos.

– [op.ext.3.1] Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro.
– [op.ext.3.2] Se estimará el riesgo sobre el sistema por causa del impacto estimado en el punto anterior.
– [op.ext.3.3] Se tomarán medidas de contención de los impactos estimados en los puntos anteriores.

Refuerzo R1-Plan de contingencia.

– [op.ext.3.r1.1] El plan de continuidad de la organización deberá tener en cuenta la dependencia de proveedores externos críticos.
– [op.ext.3.r1.2] Se deberán realizar pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor.

Refuerzo R2-Sistema de gestión de la seguridad.

– [op.ext.3.r2.1] Se implementará un sistema de protección de los procesos y flujos de información en las relaciones en línea (*online*) entre los distintos integrantes de la cadena de suministro.

Refuerzo R3-Lista de componentes software.

– [op.ext.3.r3.1] Se mantendrá actualizado un registro formal que contenga los detalles y las relaciones de la cadena de suministro de los diversos componentes utilizados en la construcción de programas informáticos, acorde a lo especificado en [mp.sw.1.r5]. Esta lista será proporcionada por el proveedor de la aplicación, librería o producto suministrado.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: no aplica.
– Categoría ALTA: op.ext.3.

4.4.4 Interconexión de sistemas [op.ext.4].

Se denomina interconexión al establecimiento de enlaces con otros sistemas de información para el intercambio de información y servicios.

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

– [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.
– [op.ext.4.2] Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.

Refuerzo R1-Coordinación de actividades.

– [op.ext.4.r1.1] Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de seguridad locales se acompañarán de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.4.
– Categoría ALTA: op.ext.4 + R1.

4.5 Servicios en la nube [op.nub].

4.5.1 Protección de servicios en la nube [op.nub.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a Service, SaaS*), Plataforma como Servicio (*Platform as a Service, PaaS*) e Infraestructura como Servicio (*Infrastructure as a Service, IaaS*) definidas en las guías CCN-STIC que sean de aplicación.
– [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

a) Auditoría de pruebas de penetración (*pentesting*).
b) Transparencia.
c) Cifrado y gestión de claves.
d) Jurisdicción de los datos.

Refuerzo R1- Servicios certificados.

– [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.
– [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Refuerzo R2-Guías de Configuración de Seguridad Específicas.

– [op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

Aplicación de la medida.

– Categoría BÁSICA: op.nub.1.
– Categoría MEDIA: op.nub.1 + R1.
– Categoría ALTA: op.nub.1+ R1 + R2.

4.6 Continuidad del servicio [op.cont].

4.6.1 Análisis de impacto [op.cont.1].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [op.cont.1.1] Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: op.cont.1.
– Nivel ALTO: op.cont.1.

4.6.2 Plan de continuidad [op.cont.2].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará los siguientes aspectos:

– [op.cont.2.1] Se identificarán funciones, responsabilidades y actividades a realizar.
– [op.cont.2.2] Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización.
– [op.cont.2.3] Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
– [op.cont.2.4] Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
– [op.cont.2.5] El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Refuerzo R1-Plan de emergencia y contingencia.

– [op.cont.2.r1.1] Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del análisis de Impacto, se determinarán los aspectos a cubrir.

Refuerzo R2-Comprobación de integridad.

– [op.cont.2.r2.1] Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.2.

4.6.3 Pruebas periódicas [op.cont.3].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

– [op.cont.3.1] Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.3.

4.6.4 Medios alternativos [op.cont.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

– [op.cont.4.1] Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto, se cubrirán los siguientes elementos del sistema:

a) Servicios contratados a terceros.
b) Instalaciones alternativas.
c) Personal alternativo.
d) Equipamiento informático alternativo.
e) Medios de comunicación alternativos.

– [op.cont.4.2] Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento.
– [op.cont.4.3] Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.

Refuerzo R1-Automatización de la transición a medios alternativos.

– [op.cont.4.r1.1] El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.4.

4.7 Monitorización del sistema [op.mon].

El sistema estará sujeto a medidas de monitorización de su actividad y ejecutará acciones predeterminadas en función de las situaciones de compromiso de la seguridad que figuren en el análisis de riesgos. Esto puede incluir la generación de alarmas en tiempo real, la finalización del proceso que está ocasionando la alarma, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

4.7.1 Detección de intrusión [op.mon.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.mon.1.1] Se dispondrá de herramientas de detección o prevención de intrusiones.

Refuerzo R1-Detección basada en reglas.

– [op.mon.1.r1.1] El sistema dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas.

Refuerzo R2-Procedimientos de respuesta.

– [op.mon.1.r2.1] Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones.

Refuerzo R3-Acciones predeterminadas.

– [op.mon.1.r3.1] El sistema ejecutará automáticamente acciones predeterminadas de respuesta a las alertas generadas. Esto puede incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.1.
– Categoría MEDIA: op.mon.1 + R1.
– Categoría ALTA: op.mon.1+ R1 + R2.

4.7.2 Sistema de métricas [op.mon.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2

Requisitos.

– [op.mon.2.1] Atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido por el artículo 32.

Refuerzo R1-Efectividad del sistema de gestión de incidentes.

– [op.mon.2.r1.1] Se recopilarán los datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de incidentes, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC.

Refuerzo R2-Eficiencia del sistema de gestión de la seguridad.

– [op.mon.2.r2.1] Se recopilarán los datos precisos para conocer la eficiencia del sistema de seguridad, en relación con los recursos consumidos, en términos de horas y presupuesto.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.2.
– Categoría MEDIA: op.mon.2 + R1+ R2.
– Categoría ALTA: op.mon.2 + R1 + R2.

4.7.3 Vigilancia [op.mon.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	+ R1+R2	+ R1+R2+R3+R4+R5+R6

Requisitos.

– [op.mon.3.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad.

Refuerzo R1-Correlación de eventos.

– [op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

Refuerzo R2-Análisis dinámico.

– [op.mon.3.r2.1] Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

Refuerzo R3-Ciberamenazas avanzadas.

– [op.mon.3.r3.1] Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos.
– [op.mon.3.r3.2] Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (*Advanced Persistent Threat, APT*) mediante la detección de anomalías significativas en el tráfico de la red.

Refuerzo R4-Observatorios digitales.

– [op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.

Refuerzo R5-Minería de datos.

Se aplicarán medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos:

– [op.mon.3.r5.1] Limitación de las consultas, monitorizando volumen y frecuencia.
– [op.mon.3.r5.2] Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.

Refuerzo R6-Inspecciones de seguridad.

Periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas, se realizarán las siguientes inspecciones:

– [op.mon.3.r6.1] Verificación de configuración.
– [op.mon.3.r6.2] Análisis de vulnerabilidades.
– [op.mon.3.r6.3] Pruebas de penetración.

Refuerzo R7-Interconexiones.

– [op.mon.3.r7.1] En las interconexiones que lo requieran se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.3.
– Categoría MEDIA: op.mon.3 + R1 + R2.
– Categoría ALTA: op.mon.3 + R1 + R2 + R3 + R4 + R5 + R6.

5. Medidas de protección [mp]

Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

5.1 Protección de las instalaciones e infraestructuras [mp.if].

5.1.1 Áreas separadas y con control de acceso [mp.if.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.if.1.1] El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas, específicas para su función.
– [mp.if.1.2] Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.1.
– Categoría MEDIA: mp.if.1.
– Categoría ALTA: mp.if.1.

5.1.2 Identificación de las personas [mp.if.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[mp.if.2.1] El procedimiento de control de acceso identificará a las personas que accedan a los locales donde hay equipamiento esencial que forme parte del sistema de información del CPD, registrando las correspondientes entradas y salidas.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.2.
– Categoría MEDIA: mp.if.2.
– Categoría ALTA: mp.if.2.

5.1.3 Acondicionamiento de los locales [mp.if.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado, y, en especial, para asegurar:

– [mp.if.3.1] Las condiciones de temperatura y humedad.
– [mp.if.3.2] La protección frente a las amenazas identificadas en el análisis de riesgos.
– [mp.if.3.3] La protección del cableado frente a incidentes fortuitos o deliberados.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.3.
– Categoría MEDIA: mp.if.3.
– Categoría ALTA: mp.if.3.

5.1.4 Energía eléctrica [mp.if.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

– [mp.if.4.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de tomas de energía eléctrica, de modo que se garantice el suministro y el correcto funcionamiento de las luces de emergencia.

Refuerzo R1-Suministro eléctrico de emergencia.

– [mp.if.4.r1.1] En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: mp.if.4.
– Nivel MEDIO: mp.if.4 + R1.
– Nivel ALTO: mp.if.4 + R1.

5.1.5 Protección frente a incendios [mp.if.5].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.if.5.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: mp.if.5.
– Nivel MEDIO: mp.if.5.
– Nivel ALTO: mp.if.5.

5.1.6 Protección frente a inundaciones [mp.if.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.if.6.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.if.6.
– Nivel ALTO: mp.if.6.

5.1.7 Registro de entrada y salida de equipamiento [mp.if.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.if.7.1] Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.7.
– Categoría MEDIA: mp.if.7.
– Categoría ALTA: mp.if.7.

5.2 Gestión del personal [mp.per].

5.2.1 Caracterización del puesto de trabajo [mp.per.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [mp.per.1.1] Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos.
– [mp.per.1.2] Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales.

Refuerzo R1-Habilitación Personal de Seguridad.

– [mp.per.1.r1.1] Los administradores de seguridad/sistema tendrán una Habilitación Personal de Seguridad (HPS) otorgada por la autoridad competente, como consecuencia de los resultados del análisis de riesgos previo o como requisito de seguridad de un sistema específico.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.per.1.
– Categoría ALTA: mp.per.1.

5.2.2 Deberes y obligaciones [mp.per.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, contemplando:

– [mp.per.2.1] Las medidas disciplinarias a que haya lugar.
– [mp.per.2.2] Contemplando tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
– [mp.per.2.3] El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.
– [mp.per.2.4] En caso de personal contratado a través de un tercero:

• [mp.per.2.4.1] Se establecerán los deberes y obligaciones de cada parte y del personal contratado.
• [mp.per.2.4.2] Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Refuerzo R1-Confirmación expresa.

– [mp.per.2.r1.1] Se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones de seguridad necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.2.
– Categoría MEDIA: mp.per.2 + R1.
– Categoría ALTA: mp.per.2 + R1.

5.2.3 Concienciación [mp.per.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:

– [mp.per.3.1] La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
– [mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
– [mp.per.3.3] El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.3.
– Categoría MEDIA: mp.per.3.
– Categoría ALTA: mp.per.3.

5.2.4 Formación [mp.per.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.per.4.1] Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:

a) Configuración de sistemas.
b) Detección y reacción ante incidentes.
c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.4.
– Categoría MEDIA: mp.per.4.
– Categoría ALTA: mp.per.4.

5.3 Protección de los equipos [mp.eq].

5.3.1 Puesto de trabajo despejado [mp.eq.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

– [mp.eq.1.1] Los puestos de trabajo permanecerán despejados, sin que exista material distinto del necesario en cada momento.

Refuerzo R1-Almacenamiento del material.

– [mp.eq.1.r1.1] Una vez usado, y siempre que sea factible, el material se almacenará en lugar cerrado.

Aplicación de la medida.

– Categoría BÁSICA: mp.eq.1.
– Categoría MEDIA: mp.eq.1 + R1.
– Categoría ALTA: mp.eq.1 + R1.

5.3.2 Bloqueo de puesto de trabajo [mp.eq.2].

dimensiones	A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

– [mp.eq.2.1] El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Refuerzo R1-Cierre de sesiones.

– [mp.eq.2.r1.1] Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

Una Guía CCN-STIC concretará la implementación de la configuración de seguridad adaptada a la categorización del sistema o perfil de cumplimiento asociado.

Aplicación de la medida (por autenticidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.eq.2.
– Nivel ALTO: mp.eq.2 + R1.

5.3.3 Protección de dispositivos portátiles [mp.eq.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+R1+R2

Requisitos.

Los equipos (ordenadores portátiles, tabletas, etc.) que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

– [mp.eq.3.1] Se llevará un inventario de dispositivos portátiles junto con una identificación de la persona responsable de cada uno de ellos y un control regular de que está positivamente bajo su control.
– [mp.eq.3.2] Se establecerá un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones.

– [mp.eq.3.3] Cuando un dispositivo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.

– [mp.eq.3.4] Se evitará, en la medida de lo posible, que el dispositivo portátil contenga claves de acceso remoto a la organización que no sean imprescindibles. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización u otras de naturaleza análoga.

Refuerzo R1– Cifrado del disco.

– [mp.eq.3.r1.1] Se protegerá el dispositivo portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO.

Refuerzo R2– Entornos protegidos.

– [mp.eq.3.r2.1] El uso de dispositivos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado y a salvo de hurtos y miradas indiscretas.

Aplicación de la medida.

– Categoría BÁSICA: mp.eq.3.
– Categoría MEDIA: mp.eq.3.
– Categoría ALTA: mp.eq.3 + R1 + R2.

5.3.4 Otros dispositivos conectados a la red [mp.eq.4].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Esta medida afecta a todo tipo de dispositivos conectados a la red y que puedan tener en algún momento acceso a la información, tales como:

a) Dispositivos multifunción: impresoras, escáneres, etc.
b) Dispositivos multimedia: proyectores, altavoces inteligentes, etc.
c) Dispositivos internet de las cosas, en inglés *Internet of Things* (*IoT*).
d) Dispositivos de invitados y los personales de los propios empleados, en inglés *Bring Your Own Device* (BYOD).
e) Otros.

Requisitos.

– [mp.eq.4.1] Los dispositivos presentes en el sistema deberán contar con una configuración de seguridad adecuada de manera que se garantice el control del flujo definido de entrada y salida de la información.

– [mp.eq.4.2] Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad necesaria para eliminar información de soportes de información. (Ver [mp.si.5]).

Refuerzo R1-Productos certificados.

– [mp.eq.4.r1.1] Se usarán, cuando sea posible, productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2-Control de dispositivos conectados a la red.

– [mp.eq.4.r2.1] Se dispondrá de soluciones que permitan visualizar los dispositivos presentes en la red, controlar su conexión/desconexión a la misma y verificar su configuración de seguridad.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.eq.4.
– Nivel MEDIO: mp.eq.4 + R1.
– Nivel ALTO: mp.eq.4+ R1.

5.4 Protección de las comunicaciones [mp.com].

5.4.1 Perímetro seguro [mp.com.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.com.1.1] Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.
– [mp.com.1.2] Todos los flujos de información a través del perímetro deben estar autorizados previamente.

La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.

Aplicación de la medida.

– Categoría BÁSICA: mp.com.1.
– Categoría MEDIA: mp.com.1.
– Categoría ALTA: mp.com.1.

5.4.2 Protección de la confidencialidad [mp.com.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+R1+R2+R3

Requisitos.

– [mp.com.2.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R1-Algoritmos y parámetros autorizados.

– [mp.com.2.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Dispositivos hardware.

– [mp.com.2.r2.1] Se emplearán, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R3-Productos certificados.

– [mp.com.2.r3.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R4-Cifradores.

– [mp.com.2.r4.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Refuerzo R5-Cifrado de información especialmente sensible.

– [mp.com.2.r5.1] Se cifrará toda la información transmitida.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.com.2.

– Nivel MEDIO: mp.com.2 + R1.
– Nivel ALTO: mp.com.2 + R1 + R2+ R3.

5.4.3 Protección de la integridad y de la autenticidad [mp.com.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4

Requisitos.

– [mp.com.3.1] En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información. (Ver [op.acc.5]).
– [mp.com.3.2] Se prevendrán ataques activos garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

a) La alteración de la información en tránsito.
b) La inyección de información espuria.
c) El secuestro de la sesión por una tercera parte.

– [mp.com.3.3] Se aceptará cualquier mecanismo de identificación y autenticación de los previstos en el ordenamiento jurídico y en la normativa de aplicación.

Refuerzo R1-Redes privadas virtuales.

– [mp.com.3.r1.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R2-Algoritmos y parámetros autorizados.

– [mp.com.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R3-Dispositivos hardware.

– [mp.com.3.r3.1] Se recomienda emplear dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R4-Productos certificados.

– [mp.com.3.r4.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R5-Cifradores.

– [mp.com.3.r5.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida (por integridad y autenticidad).

– Nivel BAJO: mp.com.3.
– Nivel MEDIO: mp.com.3 + R1 + R2.
– Nivel ALTO: mp.com.3 + R1 + R2 + R3 + R4.

5.4.4 Separación de flujos de información en la red [mp.com.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+[R1oR2oR3]	+[R2oR3]+R4

La segmentación acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.
Cuando la transmisión de información por la red se restringe a ciertos segmentos, se acota el acceso a la información y los incidentes de seguridad quedan encapsulados en su segmento.

Requisitos.

Los flujos de información se separarán en segmentos de forma que:

– [mp.com.4.1] El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita.
– [mp.com.4.2] Si se emplean comunicaciones inalámbricas, será en un segmento separado.

Refuerzo R1-Segmentación lógica básica.

– [mp.com.4.r1.1] Los segmentos de red se implementarán por medio de redes de área local virtuales (*Virtual Local Area Network, VLAN*).
– [mp.com.4.r1.2] La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo:

• Usuarios.
• Servicios.
• Administración.

Refuerzo R2-Segmentación lógica avanzada.

– [mp.com.4.r2.1] Los segmentos de red se implementarán por medio de redes privadas virtuales (*Virtual Private Network, VPN*).

Refuerzo R3-Segmentación física.

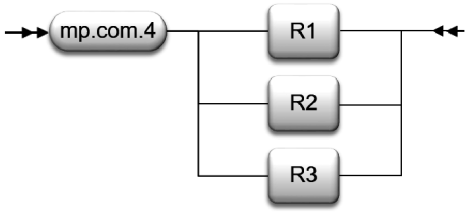
– [mp.com.4.r3.1] Los segmentos de red se implementarán con medios físicos separados.

Refuerzo R4-Puntos de interconexión.

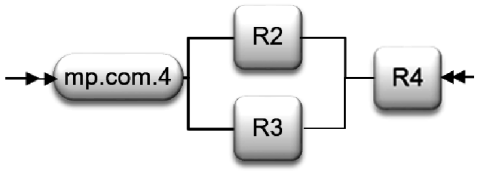
– [mp.com.4.r4.1] Control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento.
– [mp.com.4.r4.2] El punto de interconexión estará particularmente asegurado, mantenido y monitorizado, (como en [mp.com.1]).

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.com.4+ [R1o R2 o R3].



– Categoría ALTA: mp.com.4+[R2 o R3] + R4.



5.5 Protección de los soportes de información [mp.si].

5.5.1 Marcado de soportes [mp.si.1].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.si.1.1] Los soportes de información (papel impreso, documentos electrónicos, contenidos multimedia -vídeos, cursos, presentaciones- etc.) que contengan información que según [mp.info.2] deba protegerse con medidas de seguridad específicas, llevarán las marcas o metadatos correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación.

Refuerzo R1-Marca de agua digital.

– [mp.si.1.r1.1] La política de seguridad de la organización definirá marcas de agua para asegurar el uso adecuado de la información que se maneja.
– [mp.si.1.r1.2] Los soportes de información digital (documentos electrónicos, material multimedia, etc.) podrán incluir una marca de agua según la política de seguridad.
– [mp.si.1.r1.3] Los equipos o dispositivos a través de los que se accede a aplicaciones, escritorios remotos o virtuales, datos, etc., presentarán una marca de agua en pantalla según la política de seguridad.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.si.1.
– Nivel ALTO: mp.si.1.

5.5.2 Criptografía [mp.si.2].

dimensiones	C I		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1 + R2

Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, *pendrives*, memorias USB u otros de naturaleza análoga.

Requisitos.

– [mp.si.2.1] Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.
– [mp.si.2.2] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R1– Productos certificados.

– [mp.si.2.r1.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R2-Copias de seguridad.

– [mp.si.2.r2.1] Las copias se seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

Aplicación de la medida (por confidencialidad e integridad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.si.2.
– Nivel ALTO: mp.si.2 + R1 + R2.

5.5.3 Custodia [mp.si.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	aplica	aplica

Requisitos.

– [mp.si.3.1] Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) o lógicas ([mp.si.2]).
– [mp.si.3.2] Se respetarán las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agentes medioambientales.

Aplicación de la medida.

– Categoría BÁSICA: mp.si.3.
– Categoría MEDIA: mp.si.3.
– Categoría ALTA: mp.si.3.

5.5.4 Transporte [mp.si.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

El responsable del sistema garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro, fuera de las zonas controladas por la organización.

Requisitos.

– [mp.si.4.1] Se dispondrá de un registro de entrada/salida que identifique al transportista que entrega/recibe el soporte.
– [mp.si.4.2] Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.
– [mp.si.4.3] Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al mayor nivel de seguridad de la información contenida.
– [mp.si.4.4] Se gestionarán las claves según [op.exp.10].

Aplicación de la medida.

– Categoría BÁSICA: mp.si.4.
– Categoría MEDIA: mp.si.4.
– Categoría ALTA: mp.si.4.

5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos y soportes susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Requisitos.

– [mp.si.5.1] Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto del borrado seguro de su contenido que no permita su recuperación. Cuando la naturaleza del soporte no permita un borrado seguro, el soporte no podrá ser reutilizado en ningún otro sistema.

Las guías CCN-STIC del CCN precisarán los criterios para definir como seguro un mecanismo de borrado o de destrucción, en función de la sensibilidad de la información almacenada en el dispositivo.

Refuerzo R1-Productos certificados.

– [mp.si.5.r1.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2 - Destrucción de soportes.

– [mp.si.5.r2.1] Una vez finalizado el ciclo de vida del soporte de información, deberá ser destruido de forma segura conforme a los criterios establecidos por el CCN.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.si.5.
– Nivel MEDIO: mp.si.5 + R1.
– Nivel ALTO: mp.si.5 + R1.

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+R1+R2+R3+R4	+R1+R2+R3+R4

Requisitos.

– [mp.sw.1.1] El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo.

Refuerzo R1-Mínimo privilegio.

– [mp.sw.1.r1.1] Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

Refuerzo R2-Metodología de desarrollo seguro.

– [mp.sw.1.r2.1] Se aplicará una metodología de desarrollo seguro reconocida que:

a) Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
b) Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (*overflow*).
c) Tratará específicamente los datos usados en pruebas.
d) Permitirá la inspección del código fuente.

Refuerzo R3-Seguridad desde el diseño.

– [mp.sw.1.r3.1] Los siguientes elementos serán parte integral del diseño del sistema:

a) Los mecanismos de identificación y autenticación.
b) Los mecanismos de protección de la información tratada.
c) La generación y tratamiento de pistas de auditoría.

Refuerzo R4-Datos de pruebas.

– [mp.sw.1.r4.1] Preferiblemente, las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales se garantizará el nivel de seguridad correspondiente.

Refuerzo R5-Lista de componentes software.

– [mp.sw.1.r5.1] El desarrollador elaborará y mantendrá actualizada una relación formal de los componentes software de terceros empleados en la aplicación o producto. Se mantendrá un histórico de los componentes utilizados en las diferentes versiones del software. El contenido mínimo de la lista de componentes, que contendrá, al menos, la identificación del componente, el fabricante y la versión empleada, se concretará en una guía CCN-STIC del CCN.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.sw.1 + R1 + R2 + R3 + R4.
– Categoría ALTA: mp.sw.1 + R1 + R2 + R3 + R4.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

– [mp.sw.2.1] Se comprobará que:

a) Se cumplen los criterios de aceptación en materia de seguridad.
b) No se deteriora la seguridad de otros componentes del servicio.

Refuerzo R1- Pruebas.

– [mp.sw.2.r1.1] Las pruebas se realizarán en un entorno aislado (pre-producción).

Refuerzo R2-Inspección de código fuente.

– [mp.sw.2.r2.1] Se realizará una auditoría de código fuente.

Aplicación de la medida.

– Categoría BÁSICA: mp.sw.2.
– Categoría MEDIA: mp.sw.2 + R1.
– Categoría ALTA: mp.sw.2 + R1.

5.7 Protección de la información [mp.info].

5.7.1 Datos personales [mp.info.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.info.1.1] Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

Aplicación de la medida.

– Categoría BÁSICA: mp.info.1.
– Categoría MEDIA: mp.info.1.
– Categoría ALTA: mp.info.1.

5.7.2 Calificación de la información [mp.info.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.info.2.1] Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
– [mp.info.2.2] La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
– [mp.info.2.3] La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.
– [mp.info.2.4] El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
– [mp.info.2.5] El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.info.2.
– Nivel ALTO: mp.info.2.

5.7.3 Firma electrónica [mp.info.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3	+ R1+R2+R3+R4

Requisitos.

– [mp.info.3.1] Se empleará cualquier tipo de firma electrónica de los previstos en el vigente ordenamiento jurídico, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre.

Refuerzo R1-Certificados cualificados.

– [mp.info.3.r1.1] Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

Refuerzo R2-Algoritmos y parámetros autorizados.

– [mp.info.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo que resulte de aplicación.

El CCN determinará los algoritmos criptográficos que hayan sido autorizados nominalmente para su uso en el Esquema Nacional de Seguridad conforme a la Instrucción Técnica de Seguridad Criptología de empleo en el ENS.

Refuerzo R3-Verificación y validación de firma.

– [mp.info.3.r3.1] Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

Refuerzo R4-Firma electrónica avanzada basada en certificados cualificados.

– [mp.info.3.r4.1] Se usará firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo «algo que se sabe» o «algo que se es».

Refuerzo R5-Firma electrónica cualificada.

– [mp.info.3.r5.1] Se usará firma electrónica cualificada, empleando productos certificados conforme a lo establecido en [op.pl.5].

Aplicación de la medida (por integridad y autenticidad).

– Nivel BAJO: mp.info.3.
– Nivel MEDIO: mp.info.3 + R1 + R2 + R3.
– Nivel ALTO: mp.info.3 + R1 + R2 + R3 + R4.

5.7.4 Sellos de tiempo [mp.info.4].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

La utilización de sellos de tiempo exigirá adoptar las siguientes cautelas:

– [mp.info.4.1] Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
– [mp.info.4.2] Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
– [mp.info.4.3] Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte, en su caso.
– [mp.info.4.4] Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) n.º 910/2014 y normativa de desarrollo.

Refuerzo R1-Productos certificados.

– [mp.info.4.r1.1.] Se utilizarán productos certificados según [op.pl.5].
– [mp.info.4.r1.2] Se asignará una fecha y hora a un documento electrónico, conforme a lo establecido en la guía CCN-STIC Criptología de empleo en el ENS.

Aplicación de la medida (por trazabilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: mp.info.4.

5.7.5 Limpieza de documentos [mp.info.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.info.5.1] En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.info.5.
– Nivel MEDIO: mp.info.5.
– Nivel ALTO: mp.info.5.

5.7.6 Copias de seguridad [mp.info.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1 + R2

Requisitos.

– [mp.info.6.1] Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad.
– [mp.info.6.2] Los procedimientos de respaldo establecidos indicarán:

a) Frecuencia de las copias.
b) Requisitos de almacenamiento en el propio lugar.
c) Requisitos de almacenamiento en otros lugares.
d) Controles para el acceso autorizado a las copias de respaldo.

Refuerzo R1-Pruebas de recuperación.

– [mp.info.6.r1.1] Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.

Refuerzo R2-Protección de las copias de seguridad.

– [mp.info.6.r2.1] Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.
– Nivel BAJO: mp.info.6.
– Nivel MEDIO: mp.info.6+ R1.
– Nivel ALTO: mp.info.6+ R1 + R2.

5.8 Protección de los servicios [mp.s].

5.8.1 Protección del correo electrónico [mp.s.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

– [mp.s.1.1] La información distribuida por medio de correo electrónico se protegerá, tanto en el cuerpo de los mensajes como en los anexos.
– [mp.s.1.2] Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

– [mp.s.1.3] Correo no solicitado, en su expresión inglesa «*spam*».
– [mp.s.1.4] Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
– [mp.s.1.5] Código móvil de tipo micro-aplicación, en su expresión inglesa «*applet*».

Se establecerán normas de uso del correo electrónico para el personal. (Ver [org.2]). Estas normas de uso contendrán:

– [mp.s.1.6] Limitaciones al uso como soporte de comunicaciones privadas.
– [mp.s.1.7] Actividades de concienciación y formación relativas al uso del correo electrónico.

Aplicación de la medida.

– Categoría BÁSICA: mp.s.1.
– Categoría MEDIA: mp.s.1.
– Categoría ALTA: mp.s.1.

5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	+[R1oR2]	+[R1oR2]	+R2+R3

Requisitos.

Los sistemas que prestan servicios *web* deberán ser protegidos frente a las siguientes amenazas:

– [mp.s.2.1] Cuando la información requiera control de acceso se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular, tomando medidas en los siguientes aspectos:

a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
b) Se prevendrán ataques de manipulación del localizador uniforme de recursos (*Uniform Resource Locator, URL*).
c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como *cookies*.
d) Se prevendrán ataques de inyección de código.

– [mp.s.2.2] Se prevendrán intentos de escalado de privilegios.
– [mp.s.2.3] Se prevendrán ataques *de cross site scripting*.

Refuerzo R1-Auditorías de seguridad.

– [mp.s.2.r1.1] Se realizarán auditorías continuas de seguridad de «caja negra» sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción.
– [mp.s.2.r1.2] La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.

Refuerzo R2-Auditorías de seguridad avanzada.

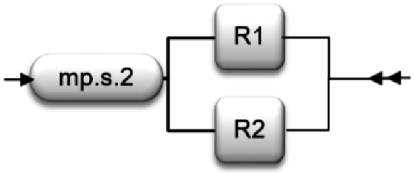
– [mp.s.2.r2.1] Se realizarán auditorías de seguridad de «caja blanca» sobre las aplicaciones web durante la fase de desarrollo.
– [mp.s.2.r2.2] Se emplearán metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías de seguridad sobre las aplicaciones web.
– [mp.s.2.r2.3] Una vez finalizada una auditoría de seguridad, se analizarán los resultados y se solventarán las vulnerabilidades encontradas mediante los procedimientos definidos [op.exp.5].

Refuerzo R3-Protección de las cachés.

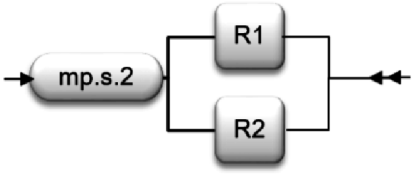
– [mp.s.2.r3.1] Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "*proxies*" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "*cachés*".

Aplicación de la medida.

– Categoría BÁSICA: mp.s.2 + [R1 o R2].



– Categoría MEDIA: mp.s.2 + [R1 o R2].



– Categoría ALTA: mp.s.2 + R2 + R3.

5.8.3 Protección de la navegación web [mp.s.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+ R1

Requisitos.

El acceso de los usuarios internos a la navegación por internet se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

– [mp.s.3.1] Se establecerá una normativa de utilización, definiendo el uso que se autoriza y las limitaciones de uso personal. En particular, se concretará el uso permitido de conexiones cifradas.
– [mp.s.3.2] Se llevarán a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos.
– [mp.s.3.3] Se formará al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes.
– [mp.s.3.4] Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.
– [mp.s.3.5] Se protegerá a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web.
– [mp.s.3.6] Se protegerá contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo *spyware*, *ransomware*, etc.
– [mp.s.3.7] Se establecerá una política ejecutiva de control de cookies, en particular, para evitar la contaminación entre uso personal y uso organizativo.

Refuerzo R1 - Monitorización.

– [mp.s.3.r1.1] Se registrará el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos.
– [mp.s.3.r1.2] Se establecerá una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones. Todo

ello sin perjuicio de que se puedan autorizar accesos cifrados singulares a destinos de confianza.

– [mp.s.3.r1.3] Se establecerá una lista negra de destinos vetados.

Refuerzo R2-Destinos autorizados.

– [mp.s.3.r2.1] Se establecerá una lista blanca de destinos accesibles. Todo acceso fuera de los lugares señalados en la lista blanca estará vetado, salvo autorización singular expresa.

Aplicación de la medida.

– Categoría BÁSICA: mp.s.3.
– Categoría MEDIA: mp.s.3.
– Categoría ALTA: mp.s.3 + R1.

5.8.4 Protección frente a la denegación de servicio [mp.s.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (*Denial of Service, DoS y Distributed Denial of Service, DDoS*). Para ello:

– [mp.s 4.1] Se planificará y dotará al sistema de capacidad suficiente para atender con holgura a la carga prevista.
– [mp.s.4.2] Se desplegarán tecnologías para prevenir los ataques conocidos.

Refuerzo R1-Detección y reacción.

– [mp.s.4.r1.1] Se establecerá un sistema de detección y tratamiento de ataques de denegación de servicio (DoS y DDoS).
– [mp.s. 4.r1.2] Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

Refuerzo R2-Ataques propios.

– [mp.s.4.r2.1] Se detectará y se evitará el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.s.4.
– Nivel ALTO: mp.s.4+ R1.

6. Valoración de la implantación de las medidas de seguridad

Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez de capacidad (*Capability Maturity Model, CMM)* permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.

Un proceso es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, proporciona un servicio para la organización.

Para la valoración de la implantación de las medidas de seguridad, estás se analizarán como procesos y se estimará su nivel de madurez usando el modelo de madurez de capacidad (CMM).

Se identifican cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez:

a) L0-Inexistente.

No existe un proceso que soporte el servicio requerido.

b) L1 - Inicial. Ad hoc.

Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.

Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

c) L2-Reproducible, pero intuitivo.

En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad.

Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

d) L3-Proceso definido.

Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

e) L4-Gestionado y medible.

Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.

f) L5 - Optimizado.

La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Para cada medida de seguridad que sea de aplicación al sistema de información se exigirá un determinado nivel de madurez. Los niveles mínimos de madurez requeridos por el ENS en función de la categoría del sistema son:

Categoría del sistema	Nivel mínimo de madurez requerido
BÁSICA	L2-Reproducible, pero intuitivo.
MEDIA	L3-Proceso definido.
ALTA	L4-Gestionado y medible.

7. Desarrollo y complemento de las medidas de seguridad

Las medidas de seguridad se desarrollarán y complementarán según lo establecido en la disposición final segunda.

8. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas de seguridad y en las guías CCN-STIC que sean de aplicación a la implementación y a los diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.

ANEXO III

Auditoría de la seguridad

1. Objeto de la auditoría

1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos, al objeto de constatar:

a) Que la política de seguridad define los roles y funciones de los responsables del sistema, la información, los servicios y la seguridad del sistema de información.
b) Que existen procedimientos para resolución de conflictos entre dichos responsables.
c) Que se han designado personas para dichos roles a la luz del principio de «diferenciación de responsabilidades».
d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, tomando como base la Declaración de Aplicabilidad regulada en el artículo 28 de este real decreto.

1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los siguientes puntos:

a) Documentación de los procedimientos.
b) Registro de incidentes.
c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en artículo 19 «Adquisición de productos de seguridad y contratación de servicios de seguridad».

1.3 Se dispondrá de un programa o plan de auditorías documentado. Las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberán ser planificadas y acordadas previamente.

2. Niveles de auditoría

Los niveles de auditoría que se realizan a los sistemas de información serán los siguientes:

2.1 Auditoría a sistemas de categoría BÁSICA.

a) Los sistemas de información de categoría BÁSICA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información o en quien éste delegue.
El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior.
b) Los informes de autoevaluación serán analizados por el responsable de la seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

2.2 Auditoría a sistemas de categoría MEDIA O ALTA.

a) El informe de auditoría dictaminará sobre el grado de cumplimiento de este real decreto e identificando los hallazgos de conformidad y no conformidad. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.
b) Los informes de auditoría serán analizados por el responsable de la seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

3. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los sistemas de información y en la guía CCN-STIC que sea de aplicación, atendiendo al espíritu y finalidad de aquellas.

ANEXO IV

Glosario

– Activo: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

– Administrador del sistema/de la seguridad del sistema: persona encargada de la instalación y el mantenimiento de un sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de la política de seguridad del organismo.

– Análisis de riesgos: estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.

– Área controlada: zona o área en la que una organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.

– Arquitectura de seguridad: conjunto de elementos físicos y lógicos que forman parte de la arquitectura del sistema y cuyo objetivo es la protección de los activos dentro del sistema y en las interconexiones con otros sistemas.

– Auditoría de la seguridad: es un proceso sistemático, independiente y documentado que persigue la obtención de evidencias objetivas y su evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios.

– Autenticación: ratificación de la identidad de un usuario, proceso o dispositivo.

– Autenticación multifactor: exigencia de dos o más factores de autenticación para ratificar una autenticación como válida.

– Autenticador: algo, físico o inmaterial, que posee el usuario bajo su exclusivo control y que le distingue de otros usuarios.

– Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Biometría (factor de autenticación): reconocimiento de los individuos en base a sus características biológicas o de comportamiento.

– Cadena de suministro: conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte. Incluye a los proveedores (primer, segundo y tercer nivel), los almacenes de materia prima (directa o indirecta), las líneas de producción, los almacenes de productos terminados y los canales de distribución (mayoristas y minoristas), hasta llegar al cliente final.

– Categoría de seguridad de un sistema: es un grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

– Certificado de firma electrónica (factor de autenticación): una declaración electrónica que vincula los datos de validación de una firma con una persona física o jurídica y confirma, al menos, el nombre o el seudónimo de esa persona.

– Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

– Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.

– Ciberataque: cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos.

– Ciberespacio: dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual.

– Ciberincidente: Incidente relacionado con la seguridad de las tecnologías de la información y las comunicaciones que se produce en el ciberespacio.

– Ciberseguridad (seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

– Compromiso de la seguridad: incidente de seguridad en el que, debido a una violación de las medidas técnicas u organizativas de seguridad, una información o un servicio quedan expuestos, o potencialmente expuestos, a un acceso no autorizado.

– Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

– Contraseña: un secreto memorizado por el usuario, compuesto por varios caracteres según unas reglas de complejidad frente a ataques de adivinación o fuerza bruta.

– Contraseña de un solo uso (*OTP - One-Time Password*): contraseña generada dinámicamente y que solamente se puede usar una vez y durante un periodo limitado.

– Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

– Dispositivo de autenticación (*token*): autenticador físico.

– Distintivo de Certificación de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado electrónicamente por la Entidad de Certificación responsable de la evaluación de los sistemas de información concernidos, incluyendo un enlace a la Certificación de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.

– Distintivo de Declaración de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado o sellado electrónicamente por la entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión, incluyendo un enlace a la Declaración de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada de que se trate.

– Dominio de seguridad: colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información. Por ejemplo:

a) Instalaciones centrales, sucursales, comerciales trabajando con portátiles.
b) Servidor central (host), frontal Unix y equipos administrativos.
c) Seguridad física, seguridad lógica.

– Evento de seguridad: ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles o una situación desconocida que puede ser relevante para la seguridad.

– Factor de autenticación: hay 3 tipos de factores de autenticación: (1) algo que se sabe, un secreto; (2) algo que se tiene, un autenticador; y (3) algo que se es, biometría.

– Firma electrónica: los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

– Firma electrónica avanzada: la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

– Firma electrónica cualificada: una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

– Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

– Gestión de riesgos: actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos.

– Incidente de seguridad (ciberincidente o incidente): suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

– Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

– Lista de componentes software: documento que detalla los componentes software utilizados para construir algo, sea una aplicación o un servicio.

– Medidas de seguridad: conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

– Mínimo privilegio: principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.

– Monitorización continua: proceso de gestión dinámica de la seguridad basado en el seguimiento de indicadores críticos de seguridad y parcheo de las vulnerabilidades descubiertas en los componentes del sistema de información.

– Observatorio Digital: un observatorio digital, en su propósito de conocer realidades de la información que se transmite a través de medios digitales, es un conjunto de capacidades para la toma de decisiones dedicado a la detección y seguimiento de anomalías en el origen, definición o diseminación de contenidos digitales, las cuales pudieran representar indicadores de amenaza.

– Perfil de cumplimiento específico: conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN.

– PIN: un secreto memorizado por el usuario, compuesto por unos pocos caracteres, siguiendo unas ciertas reglas frente a ataques de adivinación.

– Política de firma electrónica, sello electrónico y certificados: conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas y sellos electrónicos, incluyendo las características exigibles a los certificados de firma o sello electrónicos.

– Política de seguridad (Política de seguridad de la información): conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

– Principios básicos de seguridad: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

– Proceso: conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado.

– Proceso de seguridad: método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

– Proceso TIC: conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio TIC.

– Producto TIC: elemento o grupo de elementos de las redes o los sistemas de información.

– Requisitos mínimos de seguridad: exigencias mínimas necesarias para asegurar la información tratada y los servicios prestados.

– Secreto memorizado (factor de autenticación): algo que solamente sabe el usuario autorizado. Típicamente, se concreta en una contraseña o un PIN.

– Sistema de información: cualquiera de los elementos siguientes:

1.º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.

2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.

3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

– TEMPEST: término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.

– Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.

– USO OFICIAL: designa información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.

– Usuarios de la organización: personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización.

– Usuarios externos: usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados.

§ 11

Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 131, de 2 de junio de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-9175

La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, encomendó el control de la aplicación de sus disposiciones a un ente público independiente al que denominó Agencia de Protección de Datos y que se caracterizaba por la absoluta independencia de su Director en el ejercicio de sus funciones, reforzada por el establecimiento de un mandato fijo que solo podía ser acortado por un *numerus clausus* de causas de cese. La efectiva creación de la Agencia se llevó a cabo mediante la regulación de su estructura orgánica y la aprobación de su Estatuto por el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Posteriormente, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobada para transponer a nuestro Derecho la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, mantuvo la configuración de la Agencia como un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones.

En el momento actual, el régimen jurídico de la protección de datos de carácter personal viene establecido directamente por el Derecho de la Unión Europea tras la plena aplicación, desde el 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Dicho Reglamento fue adoptado con dos claros objetivos: por una parte, superar la fragmentación existente en la aplicación de las normas de trasposición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, que ha dado lugar, en la práctica, y a pesar de derivar todos ellos de unos principios comúnmente aceptados, a la existencia de tantos regímenes de protección de datos como Estados Miembros, con distintos niveles de protección y, especialmente, de reacción ante conductas que pudieran suponer una infracción de la norma. Y por otra, adaptar las normas de protección de datos a la rápida evolución tecnológica y a los fenómenos derivados del desarrollo exponencial de la sociedad de la información y la globalización que la misma conlleva en el tratamiento de los datos de carácter personal.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa, al evolucionar desde el antiguo modelo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, que estaba basado en una serie de obligaciones a las que los responsables y encargados del tratamiento habían de sujetarse, unidas al reconocimiento de potestades reactivas de las autoridades de protección de datos, hacia un nuevo paradigma basado en lo que se denomina «enfoque de riesgo»; es decir, en la necesaria evaluación por los propios responsables y encargados del tratamiento de los riesgos que su actividad puede generar en el derecho fundamental para, a partir de esa valoración, adoptar las medidas que resulten necesarias para mitigarlos en todo lo que sea posible. Se evoluciona así hacia un modelo de responsabilidad activa, que exigirá a su vez una valoración dinámica de la actividad desarrollada por el sujeto obligado por la norma y la adopción de medidas tales como la privacidad desde el diseño y por defecto, la realización de evaluaciones de impacto en la protección de datos o la implantación de medidas de seguridad técnicas y organizativas ajustadas en cada momento al estado de la técnica y a los riesgos derivados del tratamiento. En este modelo, por otra parte, las medidas de carácter organizativo, tales como la designación de un delegado de protección de datos, sobre el que recae la función de asesorar y supervisar las actividades de tratamiento de los responsables o encargados, adquieren un papel fundamental para la salvaguarda del derecho fundamental de los afectados. Finalmente, se fomenta el establecimiento de sistemas de autorregulación, incluyendo mecanismos de resolución extrajudicial de controversias, y el desarrollo de esquemas de certificación.

El nuevo modelo de protección de datos de carácter personal tiene una incidencia notable en la organización y funciones tradicionales de la Agencia Española de Protección de Datos, puesto que el Reglamento general de protección de datos refuerza las competencias de las autoridades de control que deberán contar con todos las funciones y poderes efectivos, incluidos los poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos previstos en el propio Reglamento y ha introducido los mecanismos que garanticen la necesaria coordinación y coherencia entre las diferentes autoridades de control europeas.

Para ello, el Reglamento inviste a las autoridades de protección de datos de una total independencia, destacando en el considerando 117 que «el establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa».

A estos efectos, el citado Reglamento impone a los Estados miembros la adopción de un régimen jurídico específico que deberá establecerse mediante ley respecto de todos los elementos que recoge en su artículo 54.

Para dar cumplimiento a dicha obligación se ha aprobado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, cuyo título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se han de establecer por ley nacional, configurando la Agencia Española de Protección de Datos como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

Asimismo, atribuye a la Agencia Española la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos e introduce una serie de modificaciones en su régimen jurídico con el fin de reforzar su independencia, destacando, entre otras, las relativas al procedimiento de nombramiento, mandato y cese de la Presidencia y de la Adjuntía a la Presidencia, quienes ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño; el régimen de modificaciones y de vinculación de los créditos de su presupuesto; la elaboración y aprobación de la relación de puestos de trabajo;

la composición del Consejo Consultivo; el deber de colaboración con la Agencia; la realización de planes de auditoría o las potestades de regulación por medio de circulares.

Por otro lado, hay que tener en cuenta que la Agencia Española de Protección de Datos no solo ejerce las competencias derivadas del Reglamento, sino que también ejercerá las que establece la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Igualmente ejerce actualmente las potestades derivadas de la Directiva 2002/58 del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que en la actualidad se recogen en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y en la legislación en materia de telecomunicaciones.

Por todo ello, resulta necesario la aprobación de un nuevo Estatuto que adapte la organización y funcionamiento de la Agencia Española de Protección de Datos a lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre.

El presente real decreto consta de un artículo único que aprueba el Estatuto de la Agencia Española de Protección de Datos, una disposición adicional sobre supresión de órganos directivos, una disposición transitoria única sobre unidades y puestos de trabajo con el nivel orgánico inferior a subdirección general, una disposición derogatoria única y una disposición final única relativa a la entrada en vigor del real decreto.

El Estatuto se estructura en cinco capítulos. El primero de ellos incluye las disposiciones generales sobre la naturaleza, régimen jurídico, autonomía e independencia, funciones y potestades, circulares, acción exterior, colaboración en el ámbito de la Administración de Justicia, programación, memoria anual, sede y transparencia y publicidad.

En el capítulo II se define la estructura orgánica de la Agencia Española de Protección de Datos especificando las funciones de sus diferentes órganos. En concreto, la estructura orgánica se articula en torno a la Presidencia, de la que dependen la Adjuntía a la Presidencia, la Subdirección General de Inspección de datos, la Subdirección General de Promoción y Autorizaciones, la Secretaría General, la División de Relaciones Internacionales y la División de Innovación Tecnológica. Se regula el procedimiento de designación de la Presidencia y la Adjuntía, como consecuencia de una observación formulada al respecto por el Consejo de Estado en su dictamen sobre el proyecto. También se desarrolla el régimen, competencias y funcionamiento del Consejo Consultivo en cuanto órgano colegiado de asesoramiento de la Presidencia de la Agencia Española de Protección de Datos.

El capítulo III se refiere al personal al servicio de la Agencia Española de Protección de Datos, que podrá ser funcionario o laboral, a la elaboración y aprobación de la relación de puestos de trabajo, retribuciones, evaluación del desempeño, incompatibilidades y deber de secreto profesional.

El capítulo IV regula el régimen económico, presupuestario, patrimonial y de contratación, detallando el régimen económico financiero, patrimonial y de contratación y el régimen presupuestario, de contabilidad y control económico financiero.

Por último, el capítulo V regula el asesoramiento jurídico de la Agencia, que se encomienda a la Abogacía General del Estado-Servicio Jurídico del Estado en virtud del correspondiente convenio.

Este real decreto se adecua a los principios de buena regulación (necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia) conforme a los cuales deben actuar las Administraciones Públicas en el ejercicio de la iniciativa legislativa y la potestad reglamentaria, según establece el artículo 129.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Así, este real decreto atiende a la necesidad de adecuar la estructura orgánica de la Agencia Española de Protección de Datos a lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, y en la Ley Orgánica 7/2021, de 26 de mayo, y es eficaz y proporcionado en el cumplimiento de este propósito, sin afectar en forma alguna a los derechos y deberes de la ciudadanía. Asimismo, contribuye a dotar de mayor seguridad jurídica a la organización y funcionamiento de la Agencia, al adecuarla a las nuevas competencias establecidas en

dichas normas. Cumple también con el principio de transparencia, y es también adecuada al principio de eficiencia, ya que, entre otras cuestiones, no impone cargas administrativas adicionales.

En su virtud, a propuesta de la Agencia Española de Protección de Datos, y a propuesta conjunta del Ministro de Política Territorial y Función Pública, de la Ministra de Hacienda y del Ministro de Justicia, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 1 de junio de 2021,

DISPONGO:

Artículo único. *Aprobación del Estatuto de la Agencia Española de Protección de Datos.*

De conformidad con lo dispuesto en el artículo 45.2 y en la disposición final decimoquinta de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se aprueba el Estatuto de la Agencia Española de Protección de Datos, que se inserta a continuación.

Disposición adicional única. *Supresión de órganos directivos.*

Quedan suprimidos los siguientes órganos directivos:

a) El Director de la Agencia Española de Protección de Datos.
b) El Registro General de Protección de Datos.
c) La Inspección de Datos.

Disposición transitoria única. *Unidades y puestos de trabajo con el nivel orgánico inferior a subdirección general.*

Las unidades y puestos de trabajo con el nivel orgánico inferior a subdirección general continuarán subsistentes y serán retribuidos con cargo a los mismos créditos presupuestarios hasta que se aprueben las correspondientes relaciones o catálogos de puestos de trabajo de la Agencia Española de Protección de Datos adaptados a la estructura orgánica de este real decreto.

Las unidades y puestos de trabajo encuadrados en los órganos suprimidos, o cuya dependencia orgánica haya sido modificada por este real decreto, se adscribirán provisionalmente, mediante resolución de la Presidencia de la Agencia Española de Protección de Datos, hasta tanto entren en vigor las correspondientes relaciones o catálogos de puestos de trabajo, a los órganos regulados en este real decreto en función de las atribuciones que estos tengan asignadas.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogado el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Disposición final única. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ESTATUTO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CAPÍTULO I

Disposiciones generales

Artículo 1. *Naturaleza.*

La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en el artículo 109 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Se relaciona con el Gobierno a través del Ministerio de Justicia.

Artículo 2. *Sede.*

La Agencia Española de Protección de Datos tendrá su sede en Madrid.

Artículo 3. *Régimen jurídico.*

1. La Agencia Española de Protección de Datos se rige por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, sus disposiciones de desarrollo y el presente Estatuto.

2. Supletoriamente, en cuanto sea compatible con su plena independencia, se regirá por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en particular lo dispuesto para organismos autónomos; por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; por la Ley 47/2003, de 26 de noviembre, General Presupuestaria; por la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014; por la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas, así como el resto de las normas de derecho administrativo general y especial que le sea de aplicación. En defecto de norma administrativa, se aplicará el derecho común.

3. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

4. La Agencia Española de Protección de Datos estará sujeta al principio de sostenibilidad financiera de acuerdo con lo previsto en la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

5. De conformidad con lo previsto en la disposición adicional vigésima de la Ley Orgánica 3/2018, de 5 de diciembre, no será de aplicación a la Agencia Española de Protección de Datos el artículo 50.2.c) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

6. La Agencia Española de Protección de Datos podrá adherirse a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes prevista en el artículo 95 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Artículo 4. *Autonomía e independencia.*

1. De conformidad con lo dispuesto en el artículo 52 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en el ejercicio de sus funciones y para el cumplimiento de los fines que le han sido asignados, la Agencia Española de Protección de Datos cuenta con autonomía orgánica y funcional y actúa con plena independencia del Gobierno, de las Administraciones Públicas y de cualquier interés empresarial o comercial.

2. Ni el personal ni los miembros de los órganos de la Agencia Española de Protección de Datos podrán aceptar ni solicitar instrucciones de ninguna entidad pública o privada.

Artículo 5. *Funciones y potestades.*

1. Corresponde a la Agencia Española de Protección de Datos la función de supervisar la aplicación de la normativa vigente en materia de protección de datos personales con el fin de proteger los derechos y libertades de las personas físicas en lo que respecta al tratamiento y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, y en sus disposiciones de desarrollo.

2. Asimismo, le corresponde supervisar la aplicación de la normativa vigente en materia de garantía de los derechos digitales contemplados en los artículos 89 a 94 de la Ley Orgánica 3/2018, de 5 de diciembre.

3. La Agencia Española de Protección de Datos colaborará con los órganos competentes en lo que respecta al desarrollo normativo y aplicación de las normas que incidan en materia propia del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre, y a tal efecto:

a) Informará preceptivamente los proyectos de disposiciones generales de desarrollo del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre.

b) Informará preceptivamente cualesquiera anteproyectos de ley o proyectos de reglamento que incidan en la materia propia del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre.

c) Dictará circulares que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre, así como instrucciones y recomendaciones.

4. La Agencia Española de Protección de Datos ejercerá el control de la observancia de lo dispuesto en los artículos 4, 7 y 10 a 22 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y en especial:

a) Informará con carácter preceptivo el contenido y formato de los cuestionarios, hojas censuales y otros documentos de recogida de datos con fines estadísticos.

b) Dictaminará sobre los procesos de recogida y tratamiento de los datos personales a efectos estadísticos.

c) Informará con carácter preceptivo los anteproyectos de ley por los que se exijan datos con carácter obligatorio y su adecuación a lo dispuesto en el artículo 7 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

d) Dictaminará sobre las condiciones de seguridad de los tratamientos realizados con fines exclusivamente estadísticos.

5. La Agencia Española de Protección de Datos adoptará conjuntamente con el Consejo de Transparencia y Buen Gobierno, los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma.

6. Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Artículo 6. *Circulares de la Agencia Española de Protección de Datos.*

1. La persona titular de la Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, que se denominarán «Circulares de la Agencia Española de Protección de Datos» y que serán obligatorias una vez publicadas en el «Boletín Oficial del Estado».

2. El Proyecto de Circular se iniciará mediante un informe técnico, suscrito por la persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos o el Subdirector General o Director de División correspondiente, que constará de las siguientes partes:

a) Especificación de la norma o normas habilitantes para dictar la disposición.

b) Justificación de la necesidad de la disposición, así como de las medidas o soluciones técnicas que se propongan y de los fines que se pretenden alcanzar.

c) Proyecto de Circular.

3. Se elaborará también un informe jurídico o de legalidad, emitido por el Gabinete Jurídico de la Agencia Española de Protección de Datos.

4. En el procedimiento de elaboración de las circulares se dará audiencia a las personas titulares de derechos e intereses legítimos que resulten afectados por las mismas, directamente o a través de las organizaciones y asociaciones reconocidas por la ley que los agrupen o los representen y cuyos fines guarden relación directa con el objeto de la circular, y se fomentará la participación de los ciudadanos.

El trámite de audiencia e información pública se realizará mediante la publicación del texto en la página web de la Agencia y tendrá un plazo mínimo de quince días hábiles, que podrá ser reducido hasta un mínimo de siete días hábiles cuando razones debidamente motivadas así lo justifiquen. El trámite de audiencia e información pública solo podrá omitirse cuando existan graves razones de interés público, que deberán justificarse en el informe técnico.

5. Asimismo, podrá recabarse, cuando proceda, el parecer de los departamentos de la Administración General del Estado cuyas competencias puedan verse específicamente afectadas por la regulación proyectada.

6. Cumplidos los trámites anteriores, se remitirá, cuando no le hubiera correspondido la iniciativa, a la persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos, quien podrá solicitar que se complete el expediente.

7. El proyecto de circular, acompañada de una memoria justificativa y del expediente, se elevará por la persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos quien podrá solicitar otros informes sin perjuicio de los que resulten preceptivos.

8. Se recabará el dictamen del Consejo de Estado por conducto de la persona titular del Ministerio de Justicia.

9. Una vez concluidos los trámites precedentes, el proyecto de circular será sometido a la aprobación final de la Presidencia de la Agencia Española de Protección de Datos, sin que en ningún caso sea posible la delegación de esta facultad en ningún otro órgano.

10. Las circulares serán publicadas en el «Boletín Oficial del Estado» y entrarán en vigor conforme a lo previsto en el artículo 2 del Código Civil.

Artículo 7. *Acción exterior.*

Corresponderá a la persona titular de la Presidencia de la Agencia Española de Protección de Datos designar los representantes que deban formar parte de la autoridad de control común de protección de datos prevista en los Convenios Internacionales de los que España sea parte.

Artículo 8. *Colaboración en el ámbito de la Administración de Justicia.*

La Agencia Española de Protección de Datos y el Consejo General del Poder Judicial colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos de carácter personal en el ámbito de la Administración de Justicia.

Artículo 9. *Programación.*

La Presidencia de la Agencia Española de Protección de Datos aprobará, en el primer semestre de su nombramiento y con carácter quinquenal, un Plan Estratégico con el objetivo de sentar las bases de las líneas de actuación de la Agencia en dicho periodo, incorporando las acciones específicas que cada departamento de la misma haya propuesto en relación con sus respectivas materias, así como el calendario de las circulares que se prevean aprobar.

Artículo 10. *Memoria anual.*

1. La Agencia Española de Protección de Datos redactará una Memoria anual sobre la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de las demás disposiciones legales y reglamentarias sobre protección de datos, la cual comprenderá, además de la información necesaria sobre el funcionamiento de la Agencia:

a) Una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
b) Un análisis y una valoración de los problemas de la protección de datos a escala nacional.

2. La Memoria anual se remitirá al Congreso de los Diputados, al Senado, al Gobierno, al Defensor del Pueblo y a las autoridades autonómicas de protección de datos, se pondrá a disposición de la Comisión Europea y del Comité europeo de protección de datos, y se publicará en la página web de la Agencia.

Artículo 11. *Transparencia y publicidad.*

1. La Agencia Española de Protección de Datos publicará en su página web las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, las que pongan fin a los procedimientos de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento a las entidades a que se refiere el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y las que impongan medidas cautelares.
2. Sin perjuicio de lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, será igualmente objeto de publicación en la página web toda aquella información que la Presidencia considere relevante y que contribuya al mejor cumplimiento de sus funciones.

CAPÍTULO II

Estructura orgánica de la Agencia Española de Protección de Datos

Sección 1.ª De la Presidencia de la Agencia Española de Protección de Datos

Artículo 12. *La Presidencia de la Agencia Española de Protección de Datos.*

1. La persona titular de la Presidencia de la Agencia Española de Protección de Datos tendrá la consideración de alto cargo, con rango de Subsecretario y será designada de conformidad con el procedimiento establecido en el artículo 48 de la Ley Orgánica 3/2018, de 5 de diciembre, y solo cesará por las causas que en el mismo se establecen.

2. La persona titular de la Presidencia poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

3. La persona titular de la Presidencia cesante continuará en funciones hasta la toma de posesión de la nueva persona titular de la Presidencia.

4. Es un cargo de dedicación exclusiva, está sujeto al régimen de incompatibilidades de los altos cargos de la Administración General del Estado, y será incompatible con el ejercicio de cualquier actividad pública o privada, retribuida o no, salvo las que sean inherentes a su condición de titular de la Presidencia de la Agencia Española de Protección de Datos.

5. Las retribuciones de la persona titular de la Presidencia se fijarán de acuerdo con lo dispuesto en el Real Decreto 451/2012, de 5 de marzo, por el que se regula el régimen retributivo de los máximos responsables y directivos en el sector público empresarial y otras entidades.

6. De la Presidencia depende directamente, como órgano directivo, la Adjuntía a la Presidencia.

7. Asimismo, dependen directamente de la Presidencia los siguientes órganos con nivel orgánico de subdirección general:

a) La Subdirección General de Inspección de Datos.
b) La Subdirección General de Promoción y Autorizaciones.
c) La Secretaría General.

8. También dependen directamente de la Presidencia, con el nivel que se determine en la relación de puestos de trabajo, las siguientes divisiones:

a) La División de Relaciones Internacionales.
b) La División de Innovación Tecnológica.

Artículo 13. *Funciones de la Presidencia.*

1. Corresponde a la Presidencia de la Agencia Española de Protección de Datos:

a) La dirección de la Agencia.
b) Ostentar su representación legal e institucional.
c) Aprobar las Circulares de la Agencia Española de Protección de Datos, de conformidad con lo previsto en el artículo 6 del presente Estatuto.
d) Dictar las resoluciones y directrices que requiera el ejercicio de las funciones de la Agencia, en particular las derivadas del ejercicio de las competencias previstas en el artículo 57 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y del ejercicio de los poderes de investigación y de los poderes correctivos dispuestos en el artículo 58 del citado Reglamento.
e) Acordar la realización de planes de auditoría preventiva y dictar las directrices generales o específicas que resulten de las mismas.
f) Convocar, por iniciativa propia o cuando lo solicite otra autoridad y, en todo caso, cada seis meses, a las autoridades autonómicas de protección de datos para contribuir a la aplicación coherente del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre.
g) Solicitar y facilitar a las autoridades autonómicas de protección de datos la información necesaria para el cumplimiento de sus funciones, en particular, la relativa a la actividad del Comité Europeo de Protección de Datos.
h) Requerir a las autoridades autonómicas de protección de datos cuando considere que un tratamiento llevado a cabo en materias que fueran competencia de aquellas vulnera el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, para que adopten las medidas necesarias para su cesación y ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.
i) Participar en las actividades y reuniones del Comité europeo de protección de datos como representante común del Estado español.
j) Ejercer todas aquellas funciones no atribuidas expresamente a otros órganos de la Agencia Española de Protección de Datos.

2. Asimismo, le corresponde:

a) Llevar a cabo la dirección y gestión ordinaria de la Agencia, en el marco de las funciones atribuidas en este apartado.

b) Informar al Consejo Consultivo de cuantos asuntos conciernan a los servicios a su cargo.

c) Ser órgano de contratación de la entidad.

d) Formular y aprobar las cuentas anuales de la entidad, junto con el informe de auditoría de cuentas, de conformidad con lo dispuesto en la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

e) Acordar las variaciones presupuestarias que se estimen necesarias y que no deban ser autorizadas por la persona titular del Ministerio de Hacienda y proponer aquellas que precisan autorización.

f) Autorizar, por causa justificada, la disposición de gastos, el reconocimiento de obligaciones y ordenar los pagos correspondientes y movimientos de fondos.

g) Proponer la modificación de los límites generales de compromiso de gasto con cargo a ejercicios futuros por causa justificada.

h) Suscribir, en el ámbito de sus competencias, convenios con entidades públicas y privadas.

i) Ejercer la jefatura superior del personal y prever las necesidades de personal de la Agencia Española de Protección de Datos a incorporar en la oferta anual de empleo público, en los términos previstos en el artículo 32, aprobar las relaciones de puestos de trabajo en el marco de los criterios establecidos por el Ministerio de Hacienda y la distribución del complemento de productividad y otros incentivos al rendimiento, dentro de la cantidad autorizada a estos efectos.

j) Convocar y resolver los procesos de provisión de puestos de trabajo que integren al personal de la Agencia Española de Protección de Datos y contratar al personal laboral a su servicio en los términos previstos en el artículo 34.

k) Acordar las actuaciones en materia de gestión patrimonial de la entidad.

l) La aprobación del inventario de bienes y derechos de conformidad con lo establecido en la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.

m) Las demás facultades que le atribuya el Estatuto.

Artículo 14. *Independencia.*

1. La persona titular de la Presidencia de la Agencia Española de Protección de Datos desempeñará su cargo con dedicación exclusiva, plena independencia y total objetividad.

2. La persona titular de la Presidencia no recibirá instrucciones de autoridad alguna.

Artículo 15. *Delegación de competencias.*

La Presidencia de la Agencia podrá delegar sus funciones en la Adjuntía a la Presidencia, así como en las Subdirecciones Generales que dependan directamente de la Presidencia y en la Secretaría General, en los términos previstos en el artículo 9 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

En ningún caso podrán ser objeto de delegación las funciones relacionadas con los procedimientos regulados por el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, de conformidad con el artículo 48.2. de la misma, ni la facultad para aprobar los proyectos de circulares, de acuerdo con el artículo 6.9 del presente Estatuto.

Sección 2.ª La Adjuntía a la Presidencia de la Agencia Española de Protección de Datos

Artículo 16. *Adjuntía a la Presidencia de la Agencia Española de Protección de Datos.*

1. La persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos tendrá la consideración de alto cargo, con rango de Director General.

2. La persona titular de la Adjuntía a la Presidencia será designado de conformidad con el procedimiento establecido en el artículo 48 de la Ley Orgánica 3/2018, de 5 de diciembre, y solo cesará por las causas que en el mismo se establecen.

3. La persona titular de la Adjuntía a la Presidencia poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

4. La persona titular de la Adjuntía a la Presidencia cesante continuará en funciones hasta la toma de posesión del nuevo titular.

5. La Adjuntía a la Presidencia es un cargo de dedicación exclusiva, está sujeto al régimen de incompatibilidades de los altos cargos de la Administración General del Estado, y será incompatible con el ejercicio de cualquier actividad pública o privada, retribuida o no, salvo las que sean inherentes a su condición de Adjuntía a la Presidencia de la Agencia Española de Protección de Datos.

Artículo 17. *Funciones de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos.*

Corresponderán a la persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos las siguientes competencias:

a) Ejercer las funciones de la Presidencia de la Agencia Española de Protección de Datos en los casos de delegación previstos en la Ley Orgánica 3/2018, de 5 de diciembre, y en este Estatuto. A estos efectos, la Presidencia podrá delegar sus funciones en la Adjuntía a la Presidencia, a excepción de las relacionadas con los procedimientos regulados en el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre.

b) Colaborar con la Presidencia de la Agencia Española de Protección de Datos en las relaciones con las Cortes Generales y con el Defensor del Pueblo y en la cooperación con las autoridades de control de las Comunidades Autónomas.

c) Colaborar con la Presidencia de la Agencia Española de Protección de Datos en la planificación y desarrollo de la actividad internacional de la Agencia.

d) Impulsar el procedimiento de elaboración de circulares de conformidad con lo previsto en el artículo 6 del presente Estatuto.

e) Preparar y proponer a la Presidencia de la Agencia Española de Protección de Datos el borrador del Plan estratégico y de la Memoria anual, así como el impulso y seguimiento de las actuaciones una vez aprobadas.

f) Coordinar la formación especializada de la Agencia.

g) Asumir las restantes funciones que se le encomiendan en las leyes y disposiciones reglamentarias vigentes.

Artículo 18. *Independencia.*

1. La persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos desempeñará su cargo con dedicación exclusiva, plena independencia y total objetividad.

2. Sin perjuicio de las competencias que corresponden a la Presidencia de la Agencia Española de Protección de Datos, la persona titular de la Adjuntía no recibirá instrucciones de autoridad alguna.

Sección 3.ª Procedimiento de designación de la Presidencia y la Adjuntía

Artículo 19. *Inicio del procedimiento de nombramiento y convocatoria.*

1. Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, se publicará en el «Boletín Oficial del Estado» la convocatoria pública de personas candidatas mediante orden de la persona titular del Ministerio de Justicia.

2. En la orden se regularán las bases de la convocatoria.

En ella se especificarán los requisitos a evaluar de las personas candidatas, que permitan acreditar que se trata de personas de reconocida competencia profesional, en particular en materia de protección de datos, sobre la base del mérito, la capacidad, la competencia y la idoneidad, entre los que se pueden recoger las capacidades legales de la persona candidata, la experiencia profesional, la capacidad de desarrollar el trabajo o los conocimientos técnicos, en particular referidos al ámbito de protección de datos.

3. La idoneidad de las personas candidatas exigirá que su independencia, conducta intachable e integridad deben estar fuera de toda duda.

4. Las solicitudes de participación en el procedimiento de selección se presentarán en cualquiera de los lugares previstos en el artículo 16.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 20. *Comité de selección.*

1. Una vez convocado el procedimiento, se constituirá un comité de selección con la finalidad de examinar las candidaturas y proponer la persona candidata más idónea.

2. El comité estará compuesto por:

a) La persona titular de la Secretaría de Estado de Justicia, que ostentará la Presidencia.

b) La persona titular de la Subsecretaría del Ministerio para la Presidencia, Relaciones con las Cortes y Memoria Democrática.

c) Un Magistrado o una Magistrada de la Sala Tercera del Tribunal Supremo, a propuesta del Ministerio de Justicia.

d) Un o una jurista de reconocida competencia, con al menos diez años de actividad profesional en materia de protección de datos, a propuesta del Ministerio de Justicia.

e) La persona titular de un organismo de protección de datos autonómico o una de las personas que hayan ocupado el puesto de la Dirección o Presidencia de la Agencia Española de Protección de Datos con anterioridad al saliente, a propuesta del Ministerio de Justicia.

3. La Secretaría corresponderá a un miembro de la Abogacía del Estado, designado por la persona titular de la Abogacía General del Estado-Dirección del Servicio Jurídico del Estado, que asistirá a las reuniones con voz, pero sin voto.

Los acuerdos del comité de selección se adoptarán por mayoría de sus miembros.

4. El comité de selección deberá ser paritario.

5. Podrá recabar el apoyo de las personas asesoras que estime necesarias para la correcta realización de sus funciones.

Artículo 21. *Principios aplicables al procedimiento.*

El procedimiento respetará en todas sus fases los principios de mérito, capacidad, competencia e idoneidad, así como el principio de igualdad de trato entre mujeres y hombres en el acceso al empleo público, de acuerdo con la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, y el principio de igualdad en el acceso a las funciones y cargos públicos recogido en el artículo 23.2 de la Constitución. La convocatoria respetará también los principios de igualdad y no discriminación de las personas con discapacidad.

Artículo 22. *Propuesta y comunicación de candidaturas.*

1. El comité de selección examinará las solicitudes junto con la documentación aportada y realizará, en su caso, las entrevistas oportunas.

2. Una vez valoradas las solicitudes de participación en el procedimiento de selección, el comité de selección propondrá una candidatura la Presidencia de la Agencia Española de Protección de Datos y a la Adjuntía a la Presidencia de entre aquellas que cumplan los requisitos establecidos en los artículos 12.2 y 16.3, respectivamente y atendidos los méritos y criterios de valoración establecidos en la convocatoria, junto con su informe justificativo.

La persona titular del Ministerio de Justicia elevará dicha propuesta junto con el informe del comité de selección al Consejo de Ministros.

3. El Consejo de Ministros debatirá la propuesta del comité de selección a la luz del informe y decidirá mediante acuerdo la propuesta de Presidencia y Adjuntía, que se remitirá al Congreso de los Diputados acompañada del informe justificativo.

En caso de que el Consejo de Ministros considere que la propuesta realizada por el comité de selección no resulta idónea la devolverá al comité de selección mediante acuerdo motivado, otorgándole un nuevo plazo para que formule nueva propuesta al Consejo de Ministros.

4. El acuerdo adoptado en el Consejo de Ministros con la propuesta de Presidencia y Adjuntía será publicado en el «Boletín Oficial del Estado» mediante orden de la persona titular del Ministerio de Justicia.

Sección 4.ª El Consejo Consultivo de la Agencia Española de Protección de Datos

Artículo 23. *El Consejo Consultivo.*

1. El Consejo Consultivo de la Agencia Española de Protección de Datos, con la composición que se establece en el artículo 49 de la Ley Orgánica 3/2018, de 5 de diciembre, es un órgano colegiado de asesoramiento de la Presidencia de la Agencia Española de Protección de Datos.

2. El Consejo Consultivo emitirá informe en todas las cuestiones que le someta la Presidencia de la Agencia de Protección de Datos y podrá formular propuestas en temas relacionados con las materias de competencia de esta.

Artículo 24. *Plazo y vacantes.*

1. Los miembros del Consejo Consultivo desempeñarán su cargo durante cinco años.

2. Se exceptúan de lo establecido en el apartado anterior los siguientes supuestos:

a) Nombramiento del Vocal para desempeñar la Presidencia de la Agencia de Protección de Datos o la Adjuntía a la Presidencia.

b) Renuncia anticipada del Vocal.

c) Pérdida de la condición que habilitó al Vocal para ser propuesto, en los supuestos previstos en las letras a) y b) del artículo 49 de la Ley Orgánica 3/2018, de 5 de diciembre.

d) Propuesta de cese emanada de las instituciones, órganos, corporaciones u organizaciones a las que se refiere el citado artículo.

3. Las vacantes que se produzcan en el Consejo Consultivo antes de expirar el plazo a que se refiere el apartado 1 deberán ser cubiertas dentro del mes siguiente a la fecha en que la vacante se hubiera producido, en la forma establecida por el artículo 49.3 de la Ley Orgánica 3/2018, de 5 de diciembre, y por el tiempo que reste para completar el mandato de quien causó la vacante a cubrir.

4. Los miembros del Consejo Consultivo no percibirán retribución alguna, sin perjuicio del abono de los gastos, debidamente justificados, que les ocasione el ejercicio de su función de conformidad, en su caso, con lo establecido en el Real Decreto 462/2002, de 24 de mayo, sobre indemnizaciones por razón del servicio.

Artículo 25. *Renovación del Consejo Consultivo.*

1. Antes de finalizar el mandato de los miembros del Consejo Consultivo, la persona titular del Ministerio de Justicia requerirá a las instituciones, órganos, corporaciones y organizaciones a que se refiere el artículo 49 de la Ley Orgánica 3/2018, de 5 de diciembre, a fin de que le comuniquen los nombres de las personas que propongan para un nuevo mandato en el Consejo Consultivo, lo que deberá efectuarse dentro del mes siguiente a la formulación del referido requerimiento.

2. Una vez transcurrido el plazo señalado para cumplimentar el requerimiento, la persona titular del Ministerio de Justicia procederá, sin más trámites, a nombrar como miembros del Consejo Consultivo, mediante Orden que se publicará en el «Boletín Oficial del Estado», a los propuestos, quienes tomarán posesión de su condición en la misma fecha en que expire el mandato de los miembros del Consejo anterior.

Artículo 26. *Funcionamiento.*

1. En lo no previsto en la Ley Orgánica 3/2018, de 5 de diciembre, y en el presente Estatuto, el Consejo Consultivo se regirá por lo establecido en materia de órganos colegiados por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El Consejo Consultivo adoptará sus acuerdos en sesión plenaria.

3. Actuará como Presidencia del Consejo Consultivo la Presidencia de la Agencia de Protección de Datos.

4. Desempeñará la Secretaría del Consejo Consultivo, con voz y sin voto, el titular de la Secretaría General de la Agencia de Protección de Datos. En caso de vacante, ausencia o enfermedad, desempeñará la Secretaría una persona funcionaria adscrita a la Secretaría General designado por la Presidencia de la Agencia a tal efecto.

5. El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia y, en todo caso, una vez al semestre. También se reunirá cuando así lo solicite la mayoría de sus miembros.

6. La persona que desempeñe la Secretaría convocará las reuniones del Consejo Consultivo, de orden de la Presidencia de la Agencia, y trasladará la convocatoria a los miembros del Consejo.

7. El Consejo Consultivo quedará válidamente constituido, en primera convocatoria, si están presentes la persona que actúe como Presidencia, la persona que desempeñe la Secretaría y la mitad de los miembros del Consejo, y, en segunda convocatoria, si están presentes la persona que actúe como Presidencia, la persona que desempeñe la Secretaría y la tercera parte de los miembros del Consejo.

8. Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante.

Sección 5.ª Otros órganos directamente dependientes de la Presidencia de la Agencia Española de Protección de Datos

Artículo 27. *La Subdirección General de Inspección de Datos.*

1. La Subdirección General de Inspección de Datos es el órgano administrativo, dependiente de la Presidencia de la Agencia Española de Protección de Datos, que desarrolla las competencias previstas en el artículo 57.1, letras f), g), h), i) y u) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y realiza las funciones de inspección y de instrucción necesarias para el ejercicio de los poderes de investigación establecidos en el artículo 58.1, letras a), b), d), e) y f) y de los poderes correctivos dispuestos en el artículo 58.2, letras a), b), c), d), f), g), i) y j), ambos del citado Reglamento.

2. Al objeto de cumplir los cometidos establecidos en el apartado anterior, a la Subdirección General de Inspección de Datos le corresponden las siguientes funciones:

a) La supervisión permanente del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de la Ley Orgánica 3/2018, de 5 de diciembre, y de las disposiciones que la desarrollen, por parte de los responsables y encargados de los tratamientos.

b) El ejercicio de las potestades de investigación definidas en el artículo 51 de la Ley Orgánica 3/2018, de 5 de diciembre.

c) La realización de planes de auditoría preventiva que contempla el artículo 54 de la Ley Orgánica 3/2018, de 5 de diciembre, referidos a los tratamientos de un sector concreto de actividad. A resultas de esos planes, le corresponde la propuesta a la Presidencia de la Agencia de emisión de directrices generales o específicas tendentes a asegurar la plena adaptación del sector o responsable a la normativa y a procurar la aplicación de los derechos y garantías reconocidos en el título X de la Ley Orgánica 3/2018, de 5 de diciembre, en la medida en que estos afecten a tratamientos de datos personales cuya investigación, y en su caso, propuesta de imposición de medida correctiva o sancionadora, corresponda a la Subdirección General de Inspección de Datos.

d) La tramitación de los procedimientos en caso de posible vulneración de la normativa de protección de datos conforme a lo dispuesto en el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, incluyendo las reclamaciones de los ciudadanos por falta de atención en sus solicitudes de ejercicio de los derechos contemplados en los artículos 15 al 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Corresponde a la Subdirección General de Inspección de Datos el deber de informar al reclamante sobre el curso y el resultado de la reclamación presentada ante la Agencia

Española de Protección de Datos, de acuerdo con lo dispuesto en el artículo 77.2 del citado Reglamento.

e) La evaluación de la admisibilidad a trámite de las reclamaciones que se presenten ante la Agencia Española de Protección de Datos, y la propuesta a la Presidencia de decisión sobre la admisión o inadmisión a trámite, conforme a lo establecido en el artículo 65 de la Ley Orgánica 3/2018, de 5 de diciembre.

f) El traslado de la reclamación al responsable del tratamiento o a su Delegado de Protección de Datos, o al organismo de supervisión establecido para la aplicación de los códigos de conducta, a fin de que den respuesta a la reclamación antes de resolver sobre su admisión a trámite, según lo establecido en el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre.

g) El análisis de la competencia de la Agencia Española de Protección de Datos respecto de las reclamaciones que reciba, la determinación de su carácter nacional o transfronterizo, y la remisión, cuando proceda, a la autoridad de control principal que se determine, según lo dispuesto en el artículo 66 de la Ley Orgánica 3/2018, de 5 de diciembre.

h) La realización de actuaciones previas de investigación acordadas por la Presidencia por propia iniciativa, a raíz de una reclamación, o a petición de otro órgano o autoridad de control, a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento, según lo dispuesto en el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre.

i) La instrucción del procedimiento para el ejercicio de la potestad sancionadora en caso de infracción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de la Ley Orgánica 3/2018, de 5 de diciembre, y de las normas de derecho interno que la desarrollen, conforme al régimen sancionador dispuesto en el título IX de la citada ley orgánica.

j) La propuesta a la Presidencia del acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora, según lo establecido en el artículo 68 de la Ley Orgánica 3/2018, de 5 de diciembre.

k) Durante las actuaciones previas de investigación o iniciado un procedimiento sancionador, la propuesta a la Presidencia de acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos, y en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado, conforme a lo establecido en el artículo 69 de la Ley Orgánica 3/2018, de 5 de diciembre.

l) La instrucción del procedimiento para el ejercicio de la potestad sancionadora por la comisión de las infracciones tipificadas en los artículos 38.3.c), d) e i) y 38.4.d), g) y h) de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, conforme a lo dispuesto en el artículo 43.1 de la citada Ley.

m) La instrucción del procedimiento para el ejercicio de la potestad sancionadora por la comisión de las infracciones graves del artículo 77 tipificadas en el apartado 37 y de las infracciones leves del artículo 78 tipificadas en el apartado 11 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, cuando se vulneren los derechos de los usuarios finales sobre protección de datos y privacidad reconocidos en el artículo 48, de acuerdo con lo establecido en el artículo 84.3 de la referida Ley.

n) La propuesta a la Presidencia de la Agencia de imponer aquella medida correctiva que resulte idónea en cada caso para garantizar la protección de los datos de carácter personal. Conforme a lo dispuesto en el artículo 58.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, podrá proponer que se ordene al responsable o encargado del tratamiento que atienda las solicitudes de ejercicio de los derechos del interesado, ordenar al responsable o encargado que las operaciones de tratamiento se ajusten a la normativa o se realicen de una determinada manera y dentro de un plazo especificado, que se imponga una limitación temporal o definitiva del tratamiento, incluida su prohibición o que se ordene la suspensión de flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

o) En la instrucción de los procedimientos sancionadores, de acuerdo con lo previsto en el artículo 76 de la Ley Orgánica 3/2018, de 5 de diciembre, la propuesta a la Presidencia de

imponer la sanción que se considere adecuada, que podrá ser de multa administrativa además o en lugar de las otras medidas correctivas previstas en el artículo 58.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, atendiendo a los hechos y a las circunstancias de cada caso individual y a las condiciones establecidas en el artículo 83 del citado Reglamento.

p) Respecto de las reclamaciones que gestiona, de las actuaciones de investigación que realiza y de los procedimientos sancionadores que instruye, la práctica de las notificaciones y comunicaciones que sean precisas en los actos de trámite, así como el registro de los datos pertinentes en el sistema de comunicación con las autoridades de control de la Unión Europea.

q) La gestión de registros internos de infracciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de las medidas adoptadas, según lo establecido en el artículo 57.1 u) del citado Reglamento.

r) La cooperación con las autoridades autonómicas de protección de datos que hubiesen asumido el ejercicio de las funciones establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, remitiéndoles aquellas reclamaciones que sean de su competencia conforme a lo dispuesto en el artículo 57 de la Ley Orgánica 3/2018, de 5 de diciembre.

s) La participación en la acción exterior de la Agencia Española de Protección de Datos en lo referente a las competencias de la Subdirección General. Particularmente, la cooperación con las demás autoridades de control de la Unión Europea respecto de las reclamaciones por infracción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de las actuaciones de investigación y de los procedimientos sancionadores que tramiten las autoridades de control de los Estados miembros, compartiendo información y prestando asistencia mutua, conforme a lo establecido en sus artículos 59, 60 y 61 del citado Reglamento, con el fin de garantizar la coherencia en la aplicación y ejecución del mismo.

t) Respecto de los recursos que se interpongan contra las actuaciones realizadas por la Subdirección General, la tramitación de los recursos en vía administrativa, así como la coordinación de la relación con los órganos jurisdiccionales y con los demás órganos de la Agencia que intervienen en la gestión de los recursos contencioso-administrativos.

u) La coordinación de la aplicación, en el ámbito de la Subdirección General, del sistema informático que establezca el Comité Europeo de Protección de Datos para la comunicación y compartición de la información entre las autoridades de protección de datos de la Unión Europea.

Artículo 28. *La Subdirección General de Promoción y Autorizaciones.*

Corresponde a la Subdirección General de Promoción y Autorizaciones el desarrollo de las siguientes funciones:

a) Promover la sensibilización de la ciudadanía y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de datos, en especial cuando se trate de actividades dirigidas específicamente a los niños, según lo establecido en el artículo 57.1.b del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

b) Promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, según lo dispuesto en su artículo 57.1.d.

c) Facilitar, previa solicitud, información a los ciudadanos en relación con el ejercicio de sus derechos en virtud del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, conforme a su artículo 57.1.e.

d) El registro y publicidad de los delegados de protección de datos de acuerdo con los artículos 37.7 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 34.4 de la Ley Orgánica 3/2018, de 5 de diciembre.

e) Elaborar las cláusulas contractuales tipo a que se refieren el artículo 28.8 y el artículo 46.2.d) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril

de 2016, y proponer a la Presidencia su aprobación o adopción, de acuerdo con su artículo 57.1.j).

f) Alentar la elaboración de códigos de conducta y dictaminar y proponer a la Presidencia la aprobación de los que proporcionen suficientes garantías con arreglo al artículo 40.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, conforme a su artículo 57.1 m).

g) Elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de acuerdo con su artículo 57.1.p).

h) Proponer a la Presidencia la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en virtud de su artículo 57.1.q).

i) Fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos según lo previsto en el artículo 57.1.n) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, proponer a la Presidencia la aprobación de los criterios de certificación de conformidad con el artículo 42.5 del mismo y la expedición de certificaciones; el registro de las concesiones, denegaciones o revocaciones de las acreditaciones y de las certificaciones expedidas y la realización de revisiones periódicas de las certificaciones expedidas, conforme a los artículos 43.5 y 57.1.n) y o) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y el artículo 39 de la Ley Orgánica 3/2018, de 5 de diciembre.

j) Proponer a la Presidencia la retirada de certificaciones o la orden al organismo de certificación para que retire certificaciones emitidas con arreglo a los artículos 42 y 43 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, o que no se emita una certificación cuando no se cumplan o dejen de cumplirse los requisitos para la certificación, de acuerdo con el artículo 58.2.h) del mismo.

k) Proponer a la Presidencia la autorización de las transferencias internacionales en virtud de cláusulas contractuales y acuerdos administrativos a que se refiere el artículo 46, apartado 3 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de acuerdo con su artículo. 57.1.r).

l) Proponer a la Presidencia la aprobación de normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en su artículo 57.1.s).

m) Proponer a la Presidencia la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional de acuerdo con el artículo 58.2 j) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en los supuestos de modificación de las circunstancias que determinaron el otorgamiento de la autorización o la aprobación a que se refieren los dos apartados anteriores.

n) El registro de los sistemas de exclusión publicitaria y su publicación conforme a lo dispuesto en el artículo 23.2 de la Ley Orgánica 3/2018, de 5 de diciembre.

o) Proponer a la Presidencia las excepciones a la obligación de bloqueo en los supuestos establecidos en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

p) El ejercicio de las funciones que la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno, atribuye a las Unidades de Información.

q) La gestión de las quejas y sugerencias, de conformidad con el Real Decreto 951/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

Artículo 29. *La Secretaría General de la Agencia Española de Protección de Datos.*

1. La Agencia Española de Protección de Datos contará con una Secretaría General, con nivel orgánico de subdirección general, bajo la inmediata dirección de la Presidencia, a la que corresponde tener a su cargo los servicios comunes y de carácter administrativo de la entidad.

2. La Secretaría General de la Agencia Española de Protección de Datos tendrá atribuidas las siguientes funciones:

a) Elaborar los informes y propuestas que le solicite la Presidencia.

b) Notificar las resoluciones de la Presidencia, salvo las que se dicten por delegación, que se notificarán por el órgano delegado.

c) Ejercer la Secretaría del Consejo Consultivo: Preparar los asuntos y documentación que hayan de someterse a las deliberaciones del mismo, levantar las actas de las sesiones, expedir certificaciones de los acuerdos adoptados y tramitar los acuerdos adoptados.

d) La colaboración en la preparación de conferencias, seminarios y cualesquiera otras actividades similares que organice la Agencia Española de Protección de Datos.

e) La gestión y administración de recursos humanos incluida la elaboración de la relación de puestos de trabajo, la gestión de los procesos de selección del personal laboral, la gestión de la acción social y la formación de los recursos humanos, bajo la supervisión de la Presidencia.

f) La planificación y ejecución de la política de prevención de riesgos laborales.

g) El mantenimiento de las relaciones con los órganos de participación y representación del personal.

h) La gestión de los recursos materiales de la Agencia Española de Protección de Datos, y en el ejercicio de las competencias en materia patrimonial correspondientes a la Agencia, la conservación y mantenimiento y seguridad de su patrimonio y llevar el inventario de los bienes y derechos que se integren en él.

i) El régimen interior, asuntos generales y la coordinación e inspección de las instalaciones y servicios de la Agencia.

j) La gestión económico-financiera y patrimonial de la entidad, la elaboración del anteproyecto del presupuesto anual de la Agencia Española de Protección de Datos y la tramitación de sus variaciones.

k) La tramitación de los expedientes de contratación para adquisición de bienes y servicios, así como la habilitación del material.

l) La gestión presupuestaria, de los ingresos y gastos, la realización de los cobros y pagos y la gestión de la tesorería de la Agencia.

m) Las actuaciones referentes a la gestión contable y su tramitación documental, y a la preparación de las cuentas de la entidad para su rendición y aprobación.

n) Organizar, supervisar, liquidar y controlar la recaudación en periodo voluntario de los ingresos por sanciones impuestas por la Agencia Española de Protección de Datos al amparo de los previsto por el artículo 46 de la Ley Orgánica 3/2018, de 5 de diciembre.

o) La dirección y organización de los servicios de archivo y registro de la Agencia Española de Protección de Datos.

p) El desarrollo de los sistemas de información de los servicios comunes, de los sistemas de administración electrónica, el diseño y ejecución de planes y coordinación de las actuaciones y prestación de los servicios en materia de tecnologías de la información y comunicaciones, la gestión y mantenimiento de la sede electrónica y de los sitios web, la gestión de la red interna de comunicaciones, la gestión de los medios informáticos y telemáticos y su asignación a las distintas unidades orgánicas.

En el ejercicio de estas funciones, la Secretaría General podrá optar por la utilización y el aprovechamiento de módulos y servicios comunes de administración electrónica, en los términos que se acuerden con los órganos responsables en esta materia de la Administración General del Estado.

q) Redactar, proponer y tramitar los convenios con entidades públicas y privadas a celebrar por la Presidencia de la Agencia Española de Protección de Datos.

r) El ejercicio de las competencias en materia de gestión documental, estadística, recursos documentales, biblioteca y publicaciones de la Agencia Española de Protección de Datos.

s) El diseño e implementación de un sistema de evaluación del desempeño del personal en el marco de lo establecido en la normativa vigente.

t) Ejercer las potestades administrativas derivadas de las funciones de la Agencia, así como la gestión de los asuntos horizontales que no se correspondan con competencias

específicamente atribuidas a otras unidades de la Agencia y las que le sean atribuidas por normas legales o reglamentarias.

u) Desempeñar las demás facultades y funciones que le atribuya el Estatuto y cualesquiera otras normas aplicables, así como las que le deleguen, en su caso, la Presidencia, de entre las contempladas en las letras a) a l) del apartado 2 del artículo 13.

Artículo 30. *División de Relaciones Internacionales.*

Corresponde a la División de Relaciones Internacionales:

a) Organizar y coordinar la actividad internacional de la Agencia Española de Protección de Datos en su ámbito competencial, de acuerdo con los criterios y directrices establecidos por la Presidencia de la Agencia.

b) Coordinar la participación de la Agencia Española de Protección de Datos en reuniones, organizaciones y foros internacionales, en particular en el ámbito del Comité Europeo de Protección de Datos o en otros grupos de trabajo en materia de protección de datos constituidos al amparo del Derecho de la Unión Europea.

c) Coordinar la preparación de la posición de la Agencia Española de Protección de Datos en las discusiones y negociaciones internacionales, en particular en las desarrolladas en el seno del Comité Europeo de Protección de Datos.

d) Coordinar y asesorar a los órganos de la Agencia Española de Protección de Datos de los aspectos internacionales relacionados con sus funciones, en particular los que se deriven de la actividad del Comité Europeo de Protección de Datos.

e) Elaborar informes, estudios o análisis sobre la situación o evolución en el ámbito internacional de las materias relacionadas con la protección de datos.

f) Contribuir, sin perjuicio de la competencia específica de otros órganos de la Agencia y conforme a las directrices de la Presidencia, a la coordinación de la cooperación en la acción exterior en materias relacionadas con la protección de datos con otros órganos de la Administración General del Estado y entidades del sector público estatal, así como de las comunidades autónomas, y con las entidades locales, en particular con las autoridades autonómicas de protección de datos.

g) Organizar y coordinar la participación de la Agencia Española de Protección de Datos en proyectos y actividades de carácter internacional en materia de protección de datos.

Artículo 31. *División de Innovación Tecnológica.*

Corresponde a la División de Innovación Tecnológica:

a) Asesorar a la Presidencia de la Agencia Española de Protección de Datos, como a sus distintas unidades, sobre los temas tecnológicos que tienen relevancia en la protección de datos de carácter personal, y para ello, analizar las implicaciones y alternativas del estado de arte de la tecnología y generar el conocimiento necesario para anticiparse a los cambios de la misma.

b) Impulsar la protección de datos como un factor de confianza y garantía de calidad en beneficio del desarrollo económico de la sociedad con el objeto de promover la sensibilización de responsables y ciudadanos, incluido el desarrollo y mantenimiento de herramientas de ayuda para el cumplimiento por parte de los mismos y la elaboración de guías que impulsen el cumplimiento del principio de responsabilidad activa del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en el ámbito tecnológico, según su artículo 57.1.b) y d).

c) Impulsar las medidas que garanticen la compatibilidad del desarrollo tecnológico con la privacidad asegurando los derechos de los ciudadanos según lo previsto en el artículo 57.1.i) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; en particular: el asesoramiento a emprendedores y desarrolladores tecnológicos, la realización de estudios de prospección tecnológica, informar y asesorar a los proyectos tecnológicos con implicaciones en el derecho a la protección de datos de las personas, participar en proyectos tecnológicos de ámbito internacional de interés público sobre la base del derecho de la Unión Europea o de los Estados Miembros y promover la colaboración con las Universidades con el fin de impulsar la protección de datos en proyectos y contenidos curriculares jurídicos y técnicos.

d) Gestionar el Registro de brechas de seguridad para facilitar a los responsables el cumplimiento de lo previsto en el artículo 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

e) Analizar y clasificar las brechas de seguridad y, en su caso, proponer motivadamente a la Presidencia la iniciación de una investigación cuando aprecie indicios de la comisión de una infracción.

f) Emitir informes, recomendaciones y dictámenes sobre las consultas previas realizadas por los responsables conforme al artículo 36 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en virtud de lo previsto en su artículo 57.1.l).

g) Elaborar una lista positiva y, en su caso, otra negativa de tratamientos que requieren la realización de evaluaciones de impacto según lo previsto en el artículo 57.1.k) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

CAPÍTULO III

Personal al servicio de la Agencia Española de Protección de Datos

Artículo 32. *Régimen de Personal.*

1. El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral.

2. En todo caso, el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas o en la salvaguardia de los intereses generales del Estado y de las Administraciones Públicas, corresponden exclusivamente al personal funcionario público.

3. La persona titular de la Presidencia de la Agencia Española de Protección de Datos presentará anualmente al Ministerio de Política Territorial y Función Pública la propuesta de oferta de empleo público de la Agencia, para su aprobación e inclusión independiente en la oferta de empleo público de la Administración General del Estado. Dicha propuesta tendrá en cuenta las necesidades de recursos humanos de la Agencia para el adecuado ejercicio de sus funciones.

Artículo 33. *Personal funcionario.*

1. El personal funcionario de la Agencia Española de Protección de Datos se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normas aplicables al personal funcionario de la Administración General del Estado.

2. El personal funcionario que desarrolle actividades de investigación tendrá la consideración de agentes de la autoridad en el ejercicio de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio, incluso después de haber cesado en él.

3. La Presidencia de la Agencia Española de Protección de Datos convocará y resolverá los procedimientos de provisión de puestos de trabajo de conformidad con los procedimientos de provisión establecidos en la normativa sobre función pública. Tanto las convocatorias como sus resoluciones se publicarán en el «Boletín Oficial del Estado».

Artículo 34. *Personal laboral.*

1. El personal laboral de la Agencia Española de Protección de Datos se regirá por el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, la normativa convencional aplicable en su caso, y por los preceptos del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre, que expresamente le resulten de aplicación.

2. Corresponderá a la Presidencia de la Agencia Española de Protección de Datos la celebración de los contratos de trabajo del personal laboral, que será seleccionado, en ejecución de la Oferta de Empleo Público prevista en el artículo 32, mediante convocatoria pública que, además de adecuarse a la relación de puestos de trabajo de la Agencia, se

sujetará a los principios de igualdad, mérito, capacidad y publicidad previstos por el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre, así como del acceso al empleo público de las personas con discapacidad.

Artículo 35. *Relación de puestos de trabajo.*

1. La Agencia Española de Protección Datos elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por los Ministerios de Hacienda y de Política Territorial y Función Pública, respetando el límite de gasto de personal establecido en el presupuesto.

2. Las relaciones de puestos de trabajo de la Agencia Española de Protección de Datos comprenderán de forma diferenciada:

a) Los puestos de trabajo a desempeñar por personal funcionario; y contendrá su denominación, tipo y sistema de provisión, requisitos exigidos para su desempeño; así como el nivel de destino, y, en su caso, el complemento específico que corresponden a los mismos.

b) Los puestos de trabajo a desempeñar por personal laboral, fijo o temporal, contendrá el grupo profesional, familia profesional y/o especialidad y complementos del puesto; así como las características específicas del mismo, cuando proceda, y, en su caso, los requisitos de carácter profesional necesarios para su desempeño.

Artículo 36. *Retribuciones.*

Las retribuciones del personal funcionario y laboral de la Agencia se ajustarán de acuerdo con lo dispuesto en la materia en las leyes de Presupuestos Generales del Estado.

Artículo 37. *Evaluación del desempeño.*

En el marco de la política de recursos humanos, y conforme a los principios establecidos en el Real Decreto Legislativo 5/2015, de 30 de octubre, se establecerá un sistema de evaluación que sirva de instrumento objetivo para la valoración del desempeño del puesto de trabajo, a efectos retributivos y de carrera profesional del personal al servicio de la entidad. El correspondiente sistema de evaluación permitirá valorar los rendimientos colectivos de las unidades, así como realizar una valoración individual del desempeño de cada puesto de trabajo.

Artículo 38. *Incompatibilidades del personal de la Agencia Española de Protección de Datos.*

El personal de la Agencia Española de Protección de Datos estará sujeto a la Ley 53/1984, de 26 de diciembre, de Incompatibilidades del Personal al Servicio de las Administraciones Públicas.

Artículo 39. *Deber de secreto profesional.*

El personal al servicio de la Agencia Española de Protección de Datos deberá guardar secreto, incluso después de cesar en sus funciones, sobre los datos personales que conozcan en el desempeño de sus tareas y de cuantas informaciones de naturaleza confidencial hubiera conocido en el ejercicio de aquellas.

A tal efecto, la Agencia Española de Protección de Datos elaborará una política específica para garantizar la confidencialidad de la información que no tenga el carácter de pública, dentro de la cual se integrará el Código Ético del personal al servicio de la Agencia, que será objeto de publicación en su página web.

CAPÍTULO IV

Régimen económico, presupuestario, patrimonial y de contratación

Sección 1.ª Régimen económico-financiero, patrimonial y de contratación

Artículo 40. *Recursos económicos.*

1. Los recursos económicos de la Agencia Española de Protección de Datos comprenderán:

a) Las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado.
b) Los bienes y valores que constituyen su patrimonio y los productos y rentas de dicho patrimonio.
c) Los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidas en el artículo 58 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
d) Las subvenciones y aportaciones que se concedan a su favor, procedentes de fondos específicos de la Unión Europea o de otros organismos internacionales.
e) Cualesquiera otros que legalmente puedan serle atribuidos.

2. El resultado positivo de sus ingresos se destinará por la Agencia Española de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia.

Artículo 41. *Recaudación.*

1. La gestión y recaudación de las tasas, precios públicos y cualesquiera otros recursos públicos cuya gestión esté atribuida a la Agencia Española de Protección de Datos, corresponde a dicha Autoridad, pudiendo utilizar para la efectividad de los mismos el procedimiento administrativo de apremio.
2. La Agencia Española de Protección de Datos podrá convenir con la Agencia Estatal de Administración Tributaria la gestión recaudatoria en período ejecutivo de sus recursos de derecho público en la forma prevista en el Reglamento General de Recaudación aprobado por Real Decreto 939/2005, de 29 de julio.

Artículo 42. *Patrimonio.*

1. La Agencia Española de Protección de Datos tendrá, para el cumplimiento de sus fines, un patrimonio propio e independiente del de la Administración General del Estado, integrado por el conjunto de bienes y derechos de los que sea titular.
2. La gestión y administración de los bienes y derechos propios, así como de aquellos del Patrimonio del Estado que se le adscriban para el cumplimiento de sus fines, será ejercida de acuerdo con lo señalado en este Estatuto y con lo establecido para los organismos públicos en la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.
3. Corresponde a la Presidencia de la Agencia Española de Protección de Datos acordar la adquisición por cualquier título de los bienes inmuebles y derechos que resulten necesarios para los fines de la institución, así como su uso y arrendamiento, de acuerdo con el procedimiento establecido en la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.
4. La Agencia Española de Protección de Datos formará y mantendrá actualizado su inventario de bienes y derechos, tanto de los propios como de los bienes del Patrimonio del Estado adscritos a dicha entidad, que se revisará anualmente, con referencia al 31 de diciembre, y se someterá a la aprobación de la Presidencia de la Agencia Española de Protección de Datos. El inventario y sus modificaciones se remitirán anualmente al Ministerio de Hacienda en el primer mes de cada año natural.
5. Los bienes que el Estado adscriba a la Agencia quedarán afectados a su servicio y conservarán la calificación jurídica originaria, debiendo ser utilizados exclusivamente para los fines que determinaron la adscripción.

6. La persona titular de la Presidencia podrá acordar la innecesariedad para el servicio de los bienes muebles y, en su caso, la enajenación, cesión gratuita o destrucción del material no útil, así como cualesquiera otros de igual naturaleza, aplicando su producto a los fines propios de la Agencia.

Artículo 43. *Contratación.*

1. La actividad contractual de la Agencia Española de Protección de Datos queda sujeta a la Ley 9/2017, de 8 de noviembre, así como a su normativa de desarrollo.

2. A los citados efectos, aplicará el régimen previsto en las citadas normas para las Administraciones Públicas.

3. El órgano de contratación de la Agencia Española de Protección de Datos es la Presidencia, quien podrá delegar esta competencia salvo para contratos cuyo valor estimado fuera igual o superior a 120.000 euros.

4. La Agencia podrá acordar su adhesión a sistemas de contratación centralizada o la cofinanciación conjunta de contratos con el Ministerio de Hacienda cuando de ello resultase una mayor eficiencia en la asignación de recursos.

5. La Agencia recibirá las facturas electrónicas que emitan sus proveedores a través del punto general de entrada de facturas electrónicas correspondiente a la Administración General del Estado, en los términos previstos en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

Sección 2.ª Régimen presupuestario, de contabilidad y control económico-financiero

Artículo 44. *Presupuestos.*

1. La Agencia Española de Protección de Datos elaborará y aprobará anualmente su presupuesto, con la estructura que establezca el Ministerio de Hacienda y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado.

2. El presupuesto de la Agencia tendrá carácter limitativo por su importe global y carácter estimativo para la distribución de los créditos por categorías económicas, con excepción de los correspondientes a gastos de personal que, en todo caso, tendrán carácter limitativo y vinculante por su cuantía total, y de los créditos que establezcan asignaciones identificando perceptor o beneficiario, salvo las destinadas a atender transferencias corrientes o de capital al exterior, y las atenciones protocolarias y representativas, que tendrán carácter limitativo y vinculante, cualquiera que sea el nivel de la clasificación económica al que se establezcan.

3. La ejecución y modificación del presupuesto de la Agencia Española de Protección de Datos se regirán por las disposiciones de la Ley 47/2003, de 26 de noviembre, General Presupuestaria, que le sean de aplicación. La ejecución del presupuesto de la Agencia corresponde a su Presidencia.

4. El régimen de modificaciones de los créditos del presupuesto se ajustará a lo siguiente:

a) Las modificaciones del presupuesto de la Agencia serán autorizadas por la Presidencia de la Agencia Española de Protección de Datos cuando no incrementen la cuantía global del presupuesto, salvo que afecten a los créditos para gastos de personal, en cuyo caso la autorización será competencia del titular del Ministerio de Hacienda.

b) Corresponde igualmente a la Presidencia de la Agencia Española de Protección de Datos autorizar las modificaciones presupuestarias que impliquen un incremento de hasta un tres por ciento de los créditos iniciales de su presupuesto total de gastos cuando sean consecuencia de necesidades surgidas durante el ejercicio, y siempre que no se incrementen los créditos para gastos de personal, en cuyo caso será competencia del titular del Ministerio de Hacienda.

c) Corresponde al titular del Ministerio de Hacienda autorizar las modificaciones presupuestarias que impliquen un incremento por encima del tres por ciento de los créditos iniciales del presupuesto de la Agencia y siempre que no excedan de un cinco por ciento.

d) Corresponde al Gobierno las modificaciones que impliquen un incremento por encima del cinco por ciento de los créditos iniciales del presupuesto de la Agencia.

e) Si la modificación afectase a aportaciones estatales recogidas en los Presupuestos Generales del Estado, la competencia para autorizar ambas modificaciones corresponderá a la autoridad que tuviera atribuida la modificación en el Presupuesto del Estado. Estas modificaciones no computarán a efectos de los porcentajes recogidos en las letras a) y b) anteriores.

5. La Agencia Española de Protección de Datos podrá disponer de cuentas bancarias de gestión para todo tipo de ingresos y pagos en el Banco de España y en la banca comercial.

6. La Agencia podrá adquirir compromisos de gasto que hayan de extenderse a ejercicios posteriores a aquel en que se autoricen, con los límites y previsiones que le sean establecidos por ley.

7. Se dará cuenta de las modificaciones adoptadas por la Presidencia, en función de las competencias atribuidas en el apartado 4, a la Dirección General de Presupuestos, del Ministerio de Hacienda, para su toma de razón.

Artículo 45. *Contabilidad.*

1. La Agencia deberá aplicar los principios contables públicos previstos en el artículo 122 de la Ley 47/2003, de 26 de noviembre, General Presupuestaria, así como el desarrollo de los principios y las normas establecidos en el Plan General de Contabilidad Pública, aprobado por Orden EHA/1037/2010, de 13 de abril, para lo cual contará con un sistema de información económico-financiero y presupuestario que tenga por objeto mostrar, a través de estados e informes, la imagen fiel del patrimonio, de la situación financiera, de los resultados y de la ejecución del presupuesto, que proporcione información de los costes sobre su actividad que sea suficiente para una correcta y eficiente adopción de decisiones.

2. La Intervención General de la Administración del Estado establecerá los requerimientos funcionales y, en su caso, los procedimientos informáticos que deberán observarse para cumplir lo dispuesto en el apartado anterior. En concreto, la Agencia aplicará, para la gestión contable, el sistema de información contable de la Administración General del Estado y sus organismos públicos, y suscribirá el correspondiente convenio con la Intervención General de la Administración del Estado para la utilización del sistema de apoyo a la gestión de las entidades públicas administrativas y del sistema de contabilidad analítica normalizada para organizaciones administrativas.

3. El ejercicio anual se computará por años naturales, comenzando el día 1 del mes de enero de cada año.

4. La Agencia contará con un sistema de contabilidad de gestión que permita efectuar el seguimiento del cumplimiento de los compromisos asumidos.

Artículo 46. *Cuentas anuales.*

1. La persona titular de la Presidencia formulará las cuentas anuales en un plazo de tres meses desde el cierre del ejercicio económico. Una vez auditadas por la Intervención General de la Administración del Estado, serán aprobadas dentro del primer semestre del año siguiente al que se refieran.

2. La Presidencia rendirá las cuentas anuales al Tribunal de Cuentas, por conducto de la Intervención General de la Administración del Estado, en el plazo de los siete meses siguientes a la terminación del ejercicio económico y una vez aprobadas.

Artículo 47. *Control de la gestión económico-financiera.*

1. El control externo de la gestión económico-financiera de la Agencia corresponderá al Tribunal de Cuentas, de acuerdo con su normativa específica.

2. El control interno de la gestión económico-financiera corresponderá a la Intervención General de la Administración del Estado, realizándose bajo las modalidades de control financiero permanente y de auditoría pública, en las condiciones y en los términos establecidos en la Ley 47/2003, de 26 de noviembre, a través de la Intervención Delegada en la Agencia.

CAPÍTULO V

Asesoramiento jurídico de la Agencia Española de Protección de Datos

Artículo 48. *Asistencia jurídica.*

La asistencia jurídica de la Agencia Española de Protección de Datos, consistente en el asesoramiento jurídico y en la representación y defensa en juicio, corresponde a la Abogacía General del Estado-Dirección del Servicio Jurídico del Estado, mediante la formalización del oportuno convenio en los términos previstos en la Ley 52/1997, de 27 de noviembre, de Asistencia Jurídica al Estado e Instituciones Públicas, y su normativa de desarrollo.

§ 12

Resolución de 24 de mayo de 2010, de la Agencia Española de Protección de Datos, por la que se regula el Registro Electrónico de la Agencia Española de Protección de Datos

Agencia Española de Protección de Datos
«BOE» núm. 135, de 3 de junio de 2010
Última modificación: sin modificaciones
Referencia: BOE-A-2010-8827

Las iniciativas de simplificación y modernización administrativa, que potencian el uso de medios electrónicos por parte de las Administraciones Públicas en sus relaciones con los ciudadanos han sido numerosas a lo largo de los últimos años.

En el marco de dichas iniciativas y por medio de Resolución de 12 de julio de 2006 se creó el Registro Telemático de la Agencia Española de Protección de Datos, encargado de la recepción y remisión de solicitudes, escritos y comunicaciones vinculadas al procedimiento de notificación de ficheros con datos de carácter personal para su inscripción en el Registro General de Protección de Datos mediante el formulario electrónico de Notificaciones Telemáticas a la AEPD (NOTA).

Posteriormente, la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, establece, en sus artículos 24, 25 y 26, una nueva regulación de los registros electrónicos, siendo sus preceptos desarrollados por el Título IV del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la citada Ley, que regula las condiciones de su funcionamiento.

El artículo 24.1 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, establece que las administraciones públicas crearán registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

Asimismo, el artículo 25.1 de la misma Ley prevé que las disposiciones de creación de registros electrónicos especificarán el órgano o unidad responsable de su gestión, así como la fecha y hora oficial y los días declarados como inhábiles a los efectos de cómputo de plazos. Con mayor detalle, el artículo 27 del Real Decreto 1671/2009 establece que los registros electrónicos serán creados, en el caso de Organismos Públicos, mediante Resolución de su titular, debiendo dicha Resolución respetar el contenido mínimo establecido en el apartado 2 de dicho precepto.

La disposición transitoria única de la Ley 11/2007, de 22 de junio, establece en su segundo párrafo que los registros telemáticos existentes a su entrada en vigor serán considerados registros electrónicos, regulándose por lo dispuesto en los mencionados artículos 24, 25 y 26. Este régimen resultaba ya, por tanto, de aplicación al Registro telemático de esta Agencia, creado por la ya citada Resolución de 12 de julio de 2006.

Sin embargo, el nuevo marco establecido por la Ley 11/2007 y su normativa de desarrollo y las consecuencias de la progresiva implantación y desarrollo de la Administración Electrónica, unido a las especialidades derivadas del nuevo régimen legal

creado por las citadas normas aconsejan la adopción de una nueva regulación del Registro Electrónico de la Agencia Española de Protección de Datos.

En este sentido, la disposición final tercera del Real Decreto 1671/2009, de 6 de noviembre, establece que los registros telemáticos ajustarán su funcionamiento a lo establecido en el mismo dentro de los seis meses siguientes a su entrada en vigor, lo que deberá verificarse, según establece esa disposición, mediante Orden Ministerial o, en su caso, Resolución del titular del correspondiente Organismo Público, que deberá explicitar el contenido previsto en el artículo 27 del Real Decreto.

En su virtud, dispongo:

Artículo 1. *Objeto.*

1. La presente Resolución tiene como objeto la regulación del Registro electrónico de la Agencia Española de Protección de Datos en adelante «Registro Electrónico», para la recepción y remisión, por vía electrónica, de solicitudes, escritos y comunicaciones en el ámbito de los procedimientos y actuaciones incluidos en el anexo I y en la forma prevista en el artículo 24 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la citada Ley.

2. El acceso de los interesados al Registro Electrónico estará disponible a través de la Sede Electrónica del Agencia Española de Protección de Datos en la dirección sedeagpd.gob.es y en la dirección electrónica www.agpd.es

3. El registro Electrónico será único para todos los órganos de la Agencia Española de Protección de Datos.

Artículo 2. *Ámbito del Registro Electrónico de la Agencia Española de Protección de Datos.*

1. El Registro Electrónico estará habilitado únicamente para la recepción y remisión de escritos, solicitudes y comunicaciones que se presenten por medios electrónicos respecto de los trámites y procedimientos incluidos en el anexo I de esta resolución o de la versión que figure actualizada en cada momento, en la dirección electrónica de acceso al mismo junto con los correspondientes modelos normalizados para cada caso.

2. Cualquier solicitud, escrito, comunicación o documentación presentada ante el Registro Electrónico no relacionada con los trámites y procedimientos a que se refiere el apartado anterior, será remitido a las personas, órganos o unidades destinatarias, en los términos previstos en el artículo 24.2.b) de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y en el Real Decreto 1671/2009, de 6 de noviembre, que desarrolla parcialmente la citada ley.

3. Asimismo, se podrá localizar un formulario genérico que permita la presentación de solicitudes, escritos y comunicaciones no asociados a procedimientos normalizados.

4. El Registro Electrónico podrá rechazar los documentos electrónicos que se encuentren en alguna de las circunstancias previstas en el artículo 29.1 del Real Decreto 1671/2009, de 6 de noviembre, en la forma establecida en el mismo. En su caso, la notificación al remitente se hará de conformidad con lo allí dispuesto.

Artículo 3. *Sistemas de identificación y autenticación.*

1. Las solicitudes, escritos y comunicaciones podrán ser presentados ante el Registro Electrónico por los interesados o sus representantes, en los términos definidos en los artículos 30 y siguientes de la Ley 30/1992, de 26 de noviembre.

2. El firmante del documento podrá acreditar su identidad ante el Registro Electrónico mediante firma electrónica o a través de funcionarios públicos habilitados, mediante el procedimiento previsto en el artículo 22 de la Ley 11/2007, de 22 de junio.

3. Adicionalmente, cuando estén operativos los respectivos sistemas, los documentos podrán ser presentados por representación, de acuerdo con lo dispuesto en el artículo 23 de la Ley 11/2007, de 22 de junio, y artículos 13 y 14 del Real Decreto 1671/2009, de 6 de noviembre.

4. La sede electrónica informará sobre los sistemas de representación y de autenticación y firma utilizables para la presentación de escritos ante el Registro Electrónico a través de

sus aplicaciones gestoras, con especificación, en su caso, de los servicios, procedimientos y trámites a los que sean de aplicación.

5. Cuando la representación no quede acreditada o no pueda presumirse, se requerirá dicha acreditación por la vía que corresponda.

6. Se admitirán los sistemas de firma electrónica que sean conformes con lo establecido en el artículo 10 del Real Decreto 1671/2009, de 6 de noviembre, por le que se desarrolla parcialmente la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos.

7. La identificación y firma de personas físicas mediante la utilización del documento nacional de identidad electrónico serán admitidas en todos los casos.

Artículo 4. *Voluntariedad de la presentación electrónica.*

La presentación de solicitudes, escritos y comunicaciones por medio del Registro Electrónico tendrá carácter voluntario, salvo lo previsto en el artículo 27.6 de la Ley 11/2007, de 22 de junio, siendo alternativa a la utilización de los lugares señalados en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de la Administraciones Pública y del Procedimiento Administrativo Común.

Artículo 5. *Presentación de documentos y computo de plazos.*

1. El Registro Electrónico permitirá la presentación de solicitudes, escritos y comunicaciones todos los días del año, durante las veinticuatro horas del día, sin perjuicio de las interrupciones, por el tiempo imprescindible cuando concurran razones justificadas de mantenimiento técnico u operativo, de las que se informará en el propio registro y en la sede electrónica.

2. Al efecto del cómputo de los plazos, la sede electrónica mostrará en lugar fácilmente visible la fecha y hora oficial de la sede, que será la que conste como fecha y hora de la transacción, adoptando las medidas precisas para asegurar su integridad. Las personas interesadas podrán manifestar su discrepancia respecto a dichas fecha y hora en el acto mismo de presentación de los correspondientes formularios.

3. El cómputo de plazos se realizará conforme a lo dispuesto en los apartados 3, 4 y 5 del artículo 26 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. A estos efectos el Registro se regirá por la fecha y la hora oficial española, correspondiente a la península, Ceuta, Melilla y el archipiélago balear.

4. El Registro Electrónico especificará el calendario de días inhábiles relativo a sus procedimientos y trámites, que será el que se determine en la resolución anual publicada en el «Boletín Oficial del Estado» para todo el territorio nacional por el Ministerio de la Presidencia.

5. Cuando la ineludible realización de trabajos de mantenimiento u otras razones técnicas lo requieran, podrán planificarse paradas de los sistemas informáticos que afecten o imposibiliten de forma temporal el servicio de comunicaciones telemáticas. Estas paradas serán avisadas por el propio sistema con la antelación que, en caso, resulte posible. En supuestos de interrupción no planificada en el funcionamiento del Registro Telemático, y siempre que sea posible, se comunicará dicha circunstancia.

Artículo 6. *Resguardo acreditativo de la presentación.*

El Registro Electrónico emitirá automáticamente un resguardo acreditativo de la presentación del escrito, solicitud o comunicación de que se trate, en el que constarán los datos proporcionados por la persona interesada con indicación de la fecha y hora en que tal presentación se produjo en el servidor de aquél. Dicho resguardo se configurará de forma que pueda ser impreso y su contenido se ajustara a lo establecido en el artículo 30.3 del Real Decreto 1671/2009, de 6 de noviembre.

Artículo 7. *Gestión, disponibilidad y Seguridad del Registro.*

La Secretaría General de la Agencia Española de Protección de Datos será el órgano responsable de la administración, gestión, disponibilidad y seguridad del Registro Electrónico del Agencia Española de Protección de Datos creado y regulado por la presente Resolución.

En la página de Internet de la Agencia Española de Protección de Datos, o en su sede electrónica estará disponible para consulta un resumen de los protocolos de seguridad del Registro.

El Registro Electrónico dispondrá los medios organizativos y técnicos adecuados para garantizar la interoperabilidad y seguridad de acuerdo con lo previsto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad y en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad y la normativa sobre protección de datos de carácter personal según lo previsto en el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

El Registro Electrónico observará los requisitos de accesibilidad previstos en el Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el reglamento sobre condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social. En este sentido las páginas web relacionadas con el Registro Electrónico deberán ajustarse a la prioridad 1 de la Norma UNE 139803:2004.

Artículo 8. *Requisitos de la documentación complementaría.*

Los formatos de los documentos electrónicos y de las imágenes electrónicas de los documentos serán establecidos en el marco del Esquema Nacional de Interoperabilidad. De acuerdo con los Instrumentos informáticos y vías de comunicación disponibles, podrá limitarse la extensión máxima de los documentos complementarios a presentar en una sola sesión.

La presentación de solicitudes, escritos y comunicaciones podrá incorporar como documentación complementaría:

a) Los documentos que cumplan los requisitos técnicos que se regulan en e la presente Resolución.

b) Los documentos no disponibles en formato electrónico y que, por su naturaleza, no sean susceptibles de aportación utilizando el procedimiento de copia digitalizada previsto en el artículo 35.2 de la Ley 11/2007, de 22 de junio, podrán incorporarse a través de las vías previstas en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, en el plazo de 10 días desde la presentación del correspondiente formulario electrónico. El incumplimiento de este plazo para aportación de la documentación complementaria, podrá dar lugar a su requerimiento conforma a lo dispuesto en el artículo 71 de la Ley 30/1992, de 26 de noviembre.

c) Siempre que se realice la presentación de documentos electrónicos separadamente el formulario principal, el interesado deberá mencionar el número o código de registro individualizado que permita identificar el expediente en el que haya de surtir efectos.

d) Los usuarios admiten con carácter exclusivo la responsabilidad de la custodia de los elementos necesarios para su autenticación en el acceso a estos servicios, el establecimiento de la conexión precisa y la utilización de la firma electrónica, así como de las consecuencias que pudieran derivarse del uso indebido, incorrecto o negligente de los mismos. Igualmente será responsabilidad del usuario la adecuada custodia y manejo de los ficheros que sean devueltos por el registro Electrónico como acuse de recibo.

Artículo 9. *Tratamiento de datos de carácter personal.*

Las anotaciones registrales de los asientos electrónicos efectuados en el Registro Electrónico se incorporarán al «Fichero de Entrada y Salida de Documentos» modificado en la Resolución de 24 de marzo de 2009, de la Agencia Española de Protección de Datos, por la que se crean, modifican y suprimen ficheros de datos de carácter personal de la Agencia, publicada en el BOE de 7 de abril de 2009.

Artículo 10. *Publicación de nuevos procedimientos de la Agencia Española de Protección de Datos.*

La admisión de nuevos procedimientos, trámites, preimpresos, solicitudes y modelos que en su caso sea acordada por Resolución de la Agencia Española de Protección de Datos será difundida a través de la página de Internet de la Agencia y en su sede electrónica.

Disposición transitoria.

Durante el plazo de seis meses contados desde la entrada en vigor de esta Resolución seguirá existiendo, de manera subordinada al Registro Electrónico de la Agencia Española de Protección de Datos, el Registro Telemático creado por Resolución de 12 de julio de 2006 de la Agencia Española de Protección de Datos, asociado a la aplicación de Notificación Telemática de la Agencia Española de Protección de Datos (NOTA).

Disposición derogatoria única.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Resolución.

Disposición final única. *Entrada en vigor.*

La presente Resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Procedimientos competencia de la Agencia Española de Protección de Datos admisibles a través de su Registro Electrónico

Registro General de Protección de Datos

1. Notificación de la creación, modificación o supresión de ficheros con datos de carácter personal para su inscripción en el Registro General de Protección de Datos.

Se puede realizar mediante el formulario electrónico de Notificaciones Telemáticas a la AEPD (NOTA) con certificado de firma electrónica reconocido. También se podrán enviar notificaciones de ficheros a la AEPD mediante formato XML igualmente firmadas con certificado de firma electrónica reconocido.

Las especificaciones técnicas para la remisión de notificaciones en este formato se encontrarán disponibles en la página web de la AEPD (www.agpd.es y en sedeagpd.gob.es).

Esta presentación tendrá carácter voluntario para los interesados, siendo alternativa la utilización de los Registros u oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

§ 13

Resolución de 18 de marzo de 2010, de la Agencia Española de Protección de Datos, por la que se crea la Sede Electrónica de la Agencia Española de Protección de Datos

Agencia Española de Protección de Datos
«BOE» núm. 72, de 24 de marzo de 2010
Última modificación: sin modificaciones
Referencia: BOE-A-2010-4854

La incorporación de las tecnologías de la información y de las comunicaciones a la organización y funcionamiento de las Administraciones Públicas constituye un elemento clave para la garantía de la igualdad, la eficacia y la eficiencia en el acceso de los ciudadanos a los servicios públicos.

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, ya instó a las Administraciones Públicas a impulsar el empleo de los medios electrónicos en el ejercicio de sus competencias.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, ha supuesto un salto cualitativo en la implantación de las tecnologías de la información y del conocimiento en el seno de las Administraciones Públicas al reconocer el derecho de los ciudadanos a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre. El respeto y la salvaguarda del ejercicio de este derecho implica el reconocimiento de la obligación de las Administraciones Públicas de dotarse de los medios y sistemas electrónicos adecuados.

En particular, el artículo 10 de la Ley 11/2007, de 22 de junio, regula la creación de la sede electrónica como aquella dirección electrónica disponible para los ciudadanos a través de las redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

De conformidad con el artículo 3.2 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, la sede electrónica se crea mediante orden del Ministro correspondiente o resolución del titular del organismo público, en la que deberán expresarse, como mínimo, los extremos citados por dicho precepto.

A su vez, conforme a la disposición final cuarta del Real Decreto 1671/2009, «los puntos de acceso electrónico pertenecientes a la Administración General del Estado o sus organismos públicos dependientes o vinculados en los que se desarrollan actualmente comunicaciones con terceros, propias de sede electrónica, deberán adaptarse, en el plazo de cuatro meses, contados a partir de la entrada en vigor de este Real Decreto, a lo dispuesto en el mismo para las sedes o, en su caso, subsedes, electrónicas, sin perjuicio de

lo previsto en las disposiciones transitorias primera y segunda de este Real Decreto y en la disposición final tercera de la Ley 11/2007, de 22 de junio».

En su virtud, previo informe de la Abogacía del Estado en la Agencia Española de Protección de Datos, resuelvo:

Artículo 1. *Objeto.*

La presente resolución tiene por objeto la creación de la sede electrónica de la Agencia Española de Protección de Datos (en adelante, AEPD), así como la regulación de su funcionamiento.

Artículo 2. *Creación de la sede electrónica de la AEPD y ámbito de la misma.*

1. En aplicación del artículo 10 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y del artículo 3 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, se crea la sede Electrónica de la AEPD.

Dicha sede será común a todos los órganos que integran la estructura de esta Agencia.

Artículo 3. *Dirección electrónica y acceso a la sede.*

La dirección electrónica de referencia de la sede electrónica de la AEPD es https://sedeagpd.gob.es, que será accesible directamente así como a través del portal de Internet http://www.agpd.es.

Artículo 4. *Titular y órganos encargados de la gestión y de los servicios.*

1. La titularidad de la sede electrónica de la AEPD corresponde a la AEPD.

2. El órgano encargado tanto de la gestión de la sede electrónica como de los servicios disponibles para los ciudadanos en esta sede es la Secretaría General de la AEPD.

Artículo 5. *Canales de acceso a los servicios disponibles en la sede electrónica de la AEPD.*

Los canales de acceso a los servicios disponibles en la sede electrónica de la AEPD serán:

a) Acceso electrónico, a través de Internet, según los principios de accesibilidad y usabilidad establecidos en la Ley 11/2007, de 22 de junio, en los términos dictados por la normativa vigente en cada momento, en su sede electrónica.

b) Atención presencial en las oficinas de la AEPD, sin perjuicio del acceso a través de los registros regulados en el artículo 38 de la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

c) Atención telefónica, a través del servicio que se hará constar en la propia sede electrónica y el portal de la Agencia. Al tiempo de entrada en vigor de esta Resolución, el servicio se sustenta en los teléfonos 901 100 099 y 91 266 35 17

Artículo 6. *Medios para la formulación de quejas y sugerencias.*

1. Los medios disponibles para la formulación de quejas y sugerencias en relación con el contenido, gestión y servicios ofrecidos en la sede electrónica de la AEPD serán:

a) Presencial o por correo postal en la dirección de la Agencia Española de Protección de Datos, calle Jorge Juan, 6, 28001 Madrid ,o de cualquier otro órgano administrativo, de conformidad con lo dispuesto en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre.

b) Presentación telemática a través de la sede electrónica de la AEPD

2. No se considerarán medios para la formulación de quejas y sugerencias los servicios de información y asesoramiento al ciudadano en la utilización de la sede electrónica.

Artículo 7. *Contenidos de la sede.*

1. La sede electrónica de la AEPD dispondrá del contenido y de los servicios a disposición de los ciudadanos previstos expresamente en el artículo 6 del Real Decreto 1671/2009, de 6 de noviembre.

2. Los contenidos publicados en la sede electrónica de la AEPD responderán a los criterios de seguridad e interoperabilidad que derivan de la Ley 11/2007, de 22 de junio, y de los Reales Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Disposición final. *Entrada en vigor.*

La presente resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 14

Resolución de 1 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos

Agencia Española de Protección de Datos
«BOE» núm. 227, de 22 de septiembre de 2006
Última modificación: 13 de noviembre de 2008
Referencia: BOE-A-2006-16580

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), publicada en el «Boletín Oficial del Estado» de 14 de diciembre, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

El artículo 39 de la LOPD regula el Registro General de Protección de Datos, como órgano integrado en la Agencia Española de Protección de Datos al que corresponde velar por la publicidad de los tratamientos y ficheros de datos personales existentes con la finalidad de facilitar al ciudadano el ejercicio de los derechos de acceso, rectificación, cancelación y oposición que la propia Ley le reconoce.

El derecho de consulta al Registro, regulado en el artículo 14 de la LOPD habilita a cualquier persona para conocer, de forma pública y gratuita, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del fichero.

Hasta ahora, en aplicación del citado artículo 14 de la LOPD, se han venido publicando los datos correspondientes a la identidad del responsable, la dirección ante la que pueden ejercerse los derechos de acceso, rectificación, cancelación y oposición, el nombre y la finalidad del fichero, y, en el caso de los ficheros de titularidad pública, los datos relativos a la disposición general de creación de cada uno de los ficheros inscritos en el Registro General de Protección de Datos.

Entre las funciones de la Agencia Española de Protección de Datos, de acuerdo a lo establecido en el artículo 37.1.j) de la Ley Orgánica 15/1999, se encuentra la de velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto debe publicar periódicamente una relación de dichos ficheros con la información adicional que determine el Director de la Agencia.

En consonancia con lo anterior, el artículo 7 del Real Decreto 428/1993, de 26 de marzo, establece que la Agencia Española de Protección de Datos, a efectos de dar publicidad de la existencia de ficheros con datos de carácter personal, publicará y difundirá un catálogo anual de los ficheros inscritos en el Registro General de Protección de Datos, con expresión de la información que al amparo del citado artículo 37.1.j) de la LOPD, determine el Director.

En la página web de la Agencia Española de Protección de Datos (www.agpd.es) se encuentra disponible el catálogo de ficheros inscritos en el Registro General de Protección

de Datos con el objeto de difundir y dar publicidad a la existencia de ficheros de datos de carácter personal, haciendo públicos hasta este momento los datos correspondientes a la identidad del responsable, la dirección de acceso, el nombre, la descripción y la finalidad del fichero.

Tras la aprobación de los nuevos formularios electrónicos (Sistema NOTA) por los que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, por Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, publicada en el «Boletín Oficial del Estado» número 181, de 31 de julio de 2006, se han acometido modificaciones en la infraestructura tecnológica de la Agencia que hacen posible mejorar las condiciones de la publicación de los ficheros inscritos en el Registro General de Protección de Datos regulada en el artículo 37.1.j, con el objeto de facilitar el derecho de consulta regulado en el artículo 14 de la Ley, y ampliar la información que se facilita en el catálogo de ficheros.

En su virtud, y de conformidad con lo dispuesto en el citado artículo 37.1. j) de la Ley Orgánica 15/1999, de 13 de diciembre, resuelvo:

Primero.

Aprobar la información que contiene el catálogo de ficheros con datos de carácter personal inscritos en el Registro General de Protección de Datos que se incorporará a la edición que anualmente realiza la Agencia Española de Protección de Datos en CD-ROM o en el soporte que en función de la evolución de la tecnología se determine, y cuya finalidad es facilitar al ciudadano el ejercicio de los derechos de acceso, rectificación, cancelación y oposición regulados en los artículos 14 a 16 de la LOPD.

Segundo.

Aprobar la publicación del nuevo catálogo de los ficheros con datos de carácter personal inscritos en el Registro General de Protección de Datos, que estará disponible en forma gratuita en la página web de la Agencia Española de Protección de Datos (www.agpd.es), con actualización diaria, y cuya finalidad es facilitar al ciudadano el ejercicio de los derechos de acceso, rectificación, cancelación y oposición regulados en los artículos 14 a 16 de la LOPD.

Tercero.

La información que se hace pública en los catálogos que se aprueban en los apartados primero y segundo de esta Resolución se corresponde con la información que el responsable del fichero ha notificado al Registro General de Protección de Datos en los apartados siguientes: Responsable del fichero, servicio o unidad ante el que pueden ejercitarse los derechos de oposición, acceso, rectificación y cancelación, identificación y finalidad y usos previstos del fichero, origen y procedencia de los datos, incluyendo el colectivo de personas sobre el que se obtienen los datos de carácter personal, tipos de datos, estructura y organización del fichero y, en su caso, los destinatarios de cesiones y/o transferencias internacionales de datos. Además, en el caso de los ficheros de titularidad pública, se publicarán los datos relativos a la disposición general de creación, modificación o supresión del fichero.

En el caso de responsables de ficheros que actúen como persona física, no se publicará el dato relativo a su NIF.

Cuarto.

Los datos de carácter personal incluidos en los catálogos citados en los puntos primero y segundo, no podrán ser objeto de tratamiento, ni usarse para finalidades a las previstas en el artículo 14 de la LOPD.

Queda prohibida la reproducción total o parcial de los catálogos a que se refiere la presente Resolución, incluso el volcado del contenido en cualquier soporte, sin expresa autorización de la Agencia Española de Protección de Datos.

Quinto.

En ningún caso podrá tomarse la presencia o ausencia de un fichero en estos catálogos como certificación positiva o negativa de una inscripción en el Registro General de Protección de Datos.

Sexto.

La presente Resolución entrará en vigor al día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 15

Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se crea el Registro Telemático de la Agencia Española de Protección de Datos

Agencia Española de Protección de Datos
«BOE» núm. 181, de 31 de julio de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-13848

La Agencia Española de Protección de Datos es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, y que tiene por objeto la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y sus normas de desarrollo.

El art. 35.2 de la LOPD establece que en el ejercicio de sus funciones públicas, y en defecto de lo que disponga la propia LOPD y sus disposiciones de desarrollo, la Agencia Española de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

El art. 45 de la Ley 30/1992 prevé que las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias. En igual sentido, la reforma de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común efectuada por la Ley 24/2001, de 27 de diciembre, de medidas Fiscales, Administrativas y del Orden Social, tuvo por finalidad potenciar el uso de medios electrónicos, informáticos y telemáticos por la Administración.

Las previsiones de la Ley 30/1992, de 26 de diciembre fueron desarrolladas por el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, y que fue modificado por el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

El Real Decreto 209/2003 modificó igualmente el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro, añadiendo un nuevo capítulo dedicado a la regulación de los Registros Telemáticos.

Por su parte, el artículo 4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, establece que esta ley es de aplicación al uso de la firma en el seno de las administraciones

Públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquellas y éstos entre sí o con los particulares.

Teniendo en cuenta los preceptos legales citados anteriormente, la presentación por vía telemática de solicitudes, escritos y comunicaciones requiere la creación de un registro telemático que se ocupe de la recepción y remisión de los mismos, y la especificación de los procedimientos en que dicho registro podrá ser utilizado, de acuerdo con el artículo 38, apartado 9, de la Ley 30/1992, de 26 de noviembre.

En su virtud, y de conformidad con lo dispuesto en el artículo 37.1.c) de la Ley Orgánica 5/1999, de 13 de diciembre, resuelvo:

Primero. *Objeto.*

La presente resolución tiene por objeto la creación y regulación del Registro Telemático de la Agencia Española de Protección de Datos, encargado de la recepción de y remisión de solicitudes, escritos, y comunicaciones, así como el establecimiento de los requisitos y condiciones de funcionamiento de dicho registro respecto de los trámites y procedimientos comprendidos dentro de su ámbito de aplicación.

Segundo. *Ámbito de aplicación.*

El Registro Telemático de la Agencia Española de Protección de Datos estará habilitado para los procedimientos de notificación de ficheros con datos de carácter personal para su inscripción en el Registro General de Protección de Datos mediante el formulario electrónico de Notificaciones Telemáticas a la AEPD (NOTA) con certificado de firma electrónica reconocido. También se podrán enviar notificaciones de ficheros a la AEPD mediante formato XML igualmente firmadas con certificado de firma electrónica reconocido. Las especificaciones técnicas para la remisión de notificaciones en este formato se encontrarán disponibles en la página web de la AEPD (www.agpd.es).

Esta presentación tendrá carácter voluntario para los interesados, siendo alternativa la utilización de los Registros u oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

La recepción en el Registro Telemático de la Agencia Española de Protección de Datos de solicitudes, escritos y comunicaciones que no estén incluidas en lo especificado en el ámbito de aplicación, o que hayan sido presentadas por medios diferentes al telemático no producirá ningún efecto. En estos casos, se archivarán, teniéndolas por no presentadas y comunicándolo así al remitente.

El Director de la Agencia Española de Protección de Datos podrá ordenar, mediante la oportuna resolución, la inclusión de nuevos procedimientos y trámites, para los que será válido lo dispuesto en esta Resolución, así como aprobar los modelos normalizados de obligatoria utilización para su recepción y remisión a través del Registro Telemático.

La relación actualizada de solicitudes, escritos y comunicaciones relativos a los trámites y procedimientos que puedan presentarse en el Registro Telemático de la Agencia Española de Protección de Datos figurará en la dirección electrónica de acceso al registro (www.agpd.es).

Tercero. *Creación del Registro Telemático de la Agencia Española de Protección de Datos.*

1. Se crea el Registro Telemático de la Agencia Española de Protección de Datos para la recepción y remisión de solicitudes, escritos y comunicaciones relativas a los trámites y procedimientos que se especifican en el apartado segundo de esta Resolución, que se remitan y expidan mediante firma electrónica en aplicación de lo previsto en el artículo 38.9 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. En defecto de lo que pueda disponer la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y sus disposiciones de desarrollo, resultará de aplicación lo dispuesto en el Real Decreto 263/1996, de 16 de febrero, de utilización de técnicas electrónicas, Informáticas y telemáticas por la Administración General del Estado, así como en el Real Decreto 772/1999, de 7 de mayo, que regula la presentación de

solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devoluciones de originales y el régimen de las oficinas de registro, y la Orden PRE/1551/2003, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, que regula los registros y notificaciones telemáticas, así como la utilización de los medios telemáticos para la sustitución de certificados por los ciudadanos.

3. El Registro Telemático de la Agencia Española de Protección de Datos, se configura como un registro auxiliar del Registro de Entrada y Salida de este Ente Público, en los términos previstos en el apartado 4 del artículo 7 del Real Decreto 263/1996.

4. El acceso al Registro Telemático de la Agencia Española de Protección de Datos por los interesados se realizará a través de la dirección electrónica de la Agencia (www.agpd.es).

Cuarto. *Requerimientos técnicos necesarios para el acceso al Registro Telemático de la Agencia Española de Protección de Datos.*

1. El acceso de los ciudadanos interesados en comunicarse con el Registro Telemático se realizará a través de Internet mediante el correspondiente navegador web. En la dirección electrónica de acceso al Registro Telemático estará disponible la relación de los sistemas operativos y navegadores que puedan ser utilizados por los interesados.

2. Cuando así lo prevea la norma de aprobación de los modelos utilizados para el envío y recepción de solicitudes, escritos y comunicaciones telemáticas relacionadas con los trámites y procedimientos incluidos en el ámbito del Registro Telemático, se permitirá el acceso a través de tecnologías que permitan la comunicación directa entre éste y las aplicaciones desarrolladas por los interesados o por la propia Agencia. En estos casos, la norma de aprobación de los modelos y comunicaciones telemáticas deberá especificar los formatos de intercambio de datos, y las especificaciones técnicas necesarias para el envío y recepción de los documentos.

3. De acuerdo con el principio de neutralidad tecnológica, los requisitos técnicos necesarios para el acceso al Registro Telemático de la Agencia se adecuarán en lo posible a los estándares y directrices que favorezcan su interoperabilidad y su compatibilidad con el mayor número de herramientas informáticas posible, como navegadores y sistemas operativos.

Quinto. *Sistemas de firma electrónica reconocidos.*

1. Las solicitudes, escritos y comunicaciones recibidas o remitidas por el Registro Telemático estarán firmados electrónicamente, utilizando sistemas de firma electrónica según lo previsto en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, y teniendo en cuenta las normas adicionales recogidas en el artículo 4 de la mencionada Ley. Los certificados deberán ser conformes con la recomendación UIT X.509.

2. En la dirección electrónica de acceso al Registro Telemático estará disponible la información sobre la relación de prestadores de servicios de certificación y tipos de certificados electrónicos que amparen las firmas electrónicas utilizadas en la recepción y remisión de solicitudes, escritos y comunicaciones.

Sexto. *Recepción de solicitudes y cómputo de plazos.*

1. La presentación de solicitudes, escritos y comunicaciones al Registro Telemático podrá realizarse durante las 24 horas de todos los días del año. El Registro Telemático se regirá por la fecha y hora oficial española correspondiente a la península y al archipiélago Balear, que deberá figurar visible en la dirección electrónica de acceso al Registro.

2. El Registro Telemático emitirá por el mismo medio, y utilizando los sistemas que se determinen en función del procedimiento o trámite, un mensaje de confirmación de la solicitud, escrito o comunicación en el que constarán los datos proporcionados por el interesado, junto con la acreditación de la fecha y hora en que produjo la recepción y una clave de identificación de la transmisión. El mensaje de confirmación se configurará de forma que pueda ser impreso o archivado informáticamente por el interesado y que garantizará la identidad del registro, tendrá el valor de recibo de presentación a efectos de lo dispuesto en el artículo 6.3 del Real Decreto 772/1999.

3. El usuario deberá ser advertido de que la no recepción del mensaje de confirmación, o en su caso, la recepción de un mensaje de indicación de error implica que no se ha producido la recepción del mismo, debiendo realizarse la presentación en otro momento o utilizando otros medios.

4. A los efectos del cómputo de plazo, la recepción en un día inhábil se entenderá efectuada el primer día hábil siguiente. En este caso, en el asiento de entrada se inscribirán como fecha y hora de presentación aquéllas en que se produjo efectivamente la recepción, constando como fecha y hora de entrada las cero horas y un segundo del primer día hábil siguiente.

5. El calendario de días inhábiles a efectos de este Registro Telemático será el que se determine en la resolución anual publicada en el Boletín Oficial del Estado para todo el territorio nacional por el Ministerio de Administraciones Públicas, según lo dispuesto en el artículo 48.7 de la Ley 30/1992.

6. El Registro Telemático de la Agencia Española de Protección de Datos no realizará ni anotará salidas de escritos y comunicaciones en días inhábiles.

7. Cuando la ineludible realización de trabajos de mantenimiento u otras razones técnicas lo requieran, podrán planificarse paradas de los sistemas informáticos que afecten o imposibiliten de forma temporal el servicio de comunicaciones telemáticas. Estas paradas serán avisadas por el propio sistema con la antelación que, en su caso, resulte posible. En supuestos de interrupción no planificada en el funcionamiento del Registro Telemático, y siempre que sea posible, se comunicará dicha circunstancia.

Séptimo. *Seguridad.*

1. La Secretaría General de la Agencia Española de Protección de Datos será la responsable de la seguridad del Registro Telemático de la Agencia Española de Protección de Datos.

2. En la dirección electrónica del Registro Telemático estará disponible información actualizada sobre los protocolos de seguridad del registro y de las transacciones telemáticas.

Octavo. *Accesibilidad.*

1. La Agencia Española de Protección de datos tomará las medidas necesarias para lograr un adecuado nivel de accesibilidad con el fin de que el Registro Telemático pueda ser utilizado por personas discapacitadas o de edad avanzada.

2. Las páginas web de la Agencia Española de Protección de Datos relacionadas con el Registro Telemático se adecuaran a las Directrices de Accesibilidad WAI 1.0 del W3C al menos en su nivel AA.

3. Los formularios electrónicos aprobados para su remisión al Registro Telemático o los programas que a tal efecto pudiera desarrollar la Agencia Española de Protección de Datos incorporarán un grado de accesibilidad similar en función del estado de la tecnología utilizada en cada caso.

Noveno. *Entrada en vigor.*

La presente resolución entrará en vigor el día 1 de septiembre de 2006.

§ 16

Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático

Agencia Española de Protección de Datos
«BOE» núm. 181, de 31 de julio de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-13849

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), publicada en el Boletín Oficial del Estado de 14 de diciembre, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

En su artículo 39, la LOPD prevé la existencia de un Registro General de Protección de Datos (RGPD), como órgano integrado en la Agencia Española de Protección de Datos al que corresponde velar por la publicidad de los tratamientos y ficheros de datos personales existentes con la finalidad de facilitar al ciudadano el ejercicio de los derechos que la propia Ley le reconoce.

A este fin establece la obligación de notificar los ficheros de carácter personal para su inscripción en el RGPD, a aquellas personas físicas o jurídicas, de naturaleza pública o privada, u órganos administrativos, que procedan a la creación de ficheros con datos de carácter personal, con carácter previo a la misma.

Esta obligación de notificar los ficheros implica la puesta en práctica de unos procedimientos de inscripción para poder tramitar un número creciente de notificaciones.

La notificación de ficheros al Registro está regulada en los artículos 20 y 26 de la LOPD, estableciéndose el procedimiento a través del cual se realiza la misma en el Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la derogada Ley Orgánica 5/1992, cuyos artículos 5 y 6 habilitan a la Agencia Española de Protección de Datos para elaborar modelos normalizados de solicitud de inscripción para los ficheros de titularidad pública o privada, respectivamente. El Real Decreto 1332/1994 continúa vigente, según declara expresamente la Disposición transitoria tercera de la Ley Orgánica 15/1999, en cuanto no se oponga a la misma.

Mediante Resolución de 30 de mayo de 2000, de la Agencia Española de Protección de Datos, publicada en el Boletín Oficial del Estado n.º 153, de 27 de junio de 2000, se aprobaron los modelos normalizados en soporte papel, magnético y telemático a través de

los que debe efectuarse la notificación de los ficheros y su solicitud de inscripción en el Registro General de Protección de Datos. Estos modelos reemplazaron a los establecidos en la Resolución de la Agencia Española de Protección de Datos de 22 de junio de 1994, publicada en el Boletín Oficial del Estado de 23 de junio de 1994, a fin de proceder a su adaptación a los nuevos requerimientos previstos en la LOPD.

El artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, insta a las Administraciones Públicas a promover la incorporación de técnicas electrónicas, informáticas y telemáticas en el desarrollo de su actividad y el ejercicio de sus competencias. En este sentido, y como consecuencia del compromiso de la Agencia Española de Protección de Datos con la administración electrónica, la resolución de 30 de mayo de 2000, incluía la aprobación de los modelos de notificación de ficheros en soporte magnético y telemático, así como la del programa informático de generación de notificaciones, permitiendo de ese modo la remisión de las solicitudes de inscripción en soporte informático o a través de Internet, con el requisito de la presentación convencional de la correspondiente hoja de solicitud debidamente cumplimentada y firmada.

La implantación de la administración electrónica exige que se realicen, entre otras, acciones encaminadas a la simplificación administrativa y a la adaptación normativa tendente a permitir una eficaz aplicación de las soluciones tecnológicas. A su vez, el desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan exige la generalización de la confianza de la ciudadanía en las comunicaciones telemáticas.

En este sentido, debía abordarse la incorporación de procedimientos que permitiesen la utilización de la firma electrónica en el proceso de notificación de tratamientos a través de Internet, eliminando los trámites añadidos que debían verificarse en formato papel y agilizando y facilitando el procedimiento de notificación.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, regula en su artículo 4, el empleo de la firma electrónica en el ámbito de las Administraciones Públicas. La incorporación de la firma electrónica al procedimiento de notificación electrónica de inscripción de ficheros, elimina la necesidad de la presentación convencional de la hoja de solicitud.

Además, en el Real Decreto 1553/2005, de 23 de diciembre, que regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, se establece que la firma electrónica realizada a través del documento nacional de identidad tendrá respecto a los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Por otra parte, la Agencia debe llevar a la práctica las recomendaciones incluidas en el informe sobre la simplificación de los requerimientos para la notificación que, como consecuencia del primer informe sobre implementación de la Directiva 95/46/CE, fue adoptado en el seno del Grupo de Trabajo de autoridades de protección de datos creado por el artículo 29 de esta Directiva.

En este informe se establece la conveniencia de profundizar en el régimen de excepciones de la notificación de determinados ficheros prevista en la Directiva 95/46. Si bien la LOPD establece el carácter obligatorio de la notificación de todos los ficheros, sí resulta posible establecer procedimientos que faciliten el cumplimiento de esta obligación en determinados supuestos.

Del actual sistema de información del RGPD se observa que el 35% de los ficheros de titularidad privada y el 20% de los de titularidad pública, lo que supone una tercera parte del total de ficheros declarados en el Registro, se corresponden con categorías concretas de ficheros.

Así sucede con los ficheros de clientes, recursos humanos, nóminas, comunidades de propietarios, pacientes, libro recetario de oficinas de farmacia, en relación con los ficheros de titularidad privada y con los de recursos humanos, gestión del padrón, gestión económica o control de acceso, en el caso de ficheros de titularidad pública.

Teniendo en cuenta lo anterior, se ha previsto poner a disposición de los responsables que realicen este tipo de tratamientos una serie de notificaciones ya cumplimentadas, a fin de facilitar la notificación de estos ficheros mediante el formulario electrónico.

En todo caso, las solicitudes de inscripción de ficheros deberán cumplimentarse mediante los formularios electrónicos aprobados en esta Resolución y que podrán ser presentados en soporte papel, informático o telemático. Dichos formularios estarán disponibles de forma gratuita en la página web de la AEPD (www.agpd.es).

Además se pone a disposición de los responsables un sistema de intercambio basado en mensajes en formato XML, con o sin certificado de firma electrónica, a través del que se podrán enviar notificaciones mediante la utilización de programas propios. Para ello se establecen las normas que deberán cumplir las aplicaciones desarrolladas por terceros para que puedan presentar validamente las notificaciones al RGPD.

Las hojas de solicitudes correspondientes a las notificaciones de ficheros enviadas por Internet podrán ser firmadas electrónicamente, debiendo presentarse en el Registro Telemático de la Agencia Española de Protección de Datos, de acuerdo con las normas y requisitos establecidos en la resolución por la que se crea dicho Registro Telemático.

Las notificaciones también podrán continuar enviándose por Internet sin firma electrónica, si bien, en ese caso, deberá cumplimentarse y firmarse la hoja de solicitud de inscripción generada por el formulario, que habrá de presentarse en la Agencia Española de Protección de Datos, o en cualquiera de los registros y oficinas a que se refiere el artículo 38.4 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Por último, mediante el formulario electrónico NOTA se podrán presentar notificaciones en formato papel, con la seguridad de que han sido correctamente cumplimentadas. Este formato de presentación incluye un código óptico de lectura para agilizar su inscripción en el RGPD.

Cuando las notificaciones hayan sido presentadas a través de Internet mediante certificado de firma electrónica reconocido, y así lo manifiesten los interesados expresamente en el formulario de notificación, podrán recibir por medios telemáticos la notificación de la resolución de inscripción, para lo que deberán disponer de una dirección electrónica a efectos de notificaciones del Servicio de Notificaciones Telemáticas Seguras.

Adicionalmente, los interesados que hayan presentado las notificaciones a través de Internet podrán consultar el estado de tramitación de su solicitud a través de la web de la AEPD.

Con los nuevos formularios electrónicos de Notificaciones Telemáticas a la AEPD (NOTA) se incorporan nuevos servicios electrónicos para facilitar el cumplimiento del trámite de notificación, al incorporar la posibilidad de su presentación telemática con firma electrónica, y que simplifican los modelos anteriores, mejorando los requisitos de accesibilidad y de independencia de plataforma informática.

Con el fin de que los responsables de ficheros puedan adaptarse a los nuevos formularios y teniendo en cuenta la amplia difusión y aceptación del programa de ayuda para la generación de notificaciones, se considera adecuado el establecimiento de un período transitorio durante el cual seguirán siendo válidos los modelos que preveía la Resolución de 30 de mayo de 2000, sin perjuicio de que sea también ya posible la presentación en los formularios que en la presente resolución se establecen. Este período concluirá, en cuanto a la presentación de notificaciones en soporte papel, el 1 de diciembre de 2006, a fin de garantizar el uso de medios electrónicos y telemáticos en el procedimiento.

Asimismo, a fin de garantizar la homogeneidad del Registro, se procederá a la adaptación de las inscripciones actualmente existentes y las que sean presentadas conforme a los modelos previstos en la Resolución de 30 de mayo de 2000 a los requerimientos derivados de esta Resolución.

Debe recordarse que la notificación de los ficheros en el Registro General de Protección de Datos tiene un carácter declarativo y la inscripción de un fichero en el RGPD, únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en la Ley Orgánica 15/1999, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en dicha Ley y demás disposiciones reglamentarias.

En su virtud, y de conformidad con lo dispuesto en el artículo 37.1.c de la Ley Orgánica 15/1999, de 13 de diciembre, resuelvo:

Primero.

Aprobar los formularios electrónicos NOTA a través de los que deberán efectuarse las solicitudes de inscripción en el Registro General de Protección de Datos. Dichos formularios estarán disponibles de forma gratuita en la página web de la Agencia Española de Protección de Datos (www.agpd.es), figurando su copia impresa en el anexo I de la presente Resolución.

Segundo.

Aprobar las normas de cumplimentación a las que habrán de adecuarse las notificaciones de ficheros de titularidad pública y privada en el Registro General de Protección de Datos y que figuran en el anexo II de esta Resolución.

Los formularios electrónicos de notificación de ficheros a la AEPD del sistema NOTA serán dinámicos y dispondrán de la correspondiente ayuda con el fin de facilitar su cumplimentación por el declarante.

En el caso de las inscripciones de alta de ficheros se mostrarán todos los apartados que definen el fichero, si bien únicamente deberán cumplimentarse los que correspondan en función del fichero objeto de la notificación.

En el caso de modificaciones, sólo se mostrarán aquellos apartados que el declarante haya señalado como objeto de la modificación.

En el caso de las supresiones, se mostrará el apartado correspondiente en el que deberá indicarse el motivo de la supresión y el destino que se dará a los datos o las previsiones que van a adoptarse para su destrucción.

Tanto para notificar una modificación como una supresión de la inscripción deberá hacerse constar en el formulario el código de inscripción asignado por la Agencia, así como los datos identificativos del responsable del fichero que figuran en la inscripción del mismo.

Tercero.

Las notificaciones, una vez cumplimentadas mediante el formulario electrónico de Notificaciones Telemáticas a la AEPD (NOTA), podrán remitirse a la Agencia Española de Protección de Datos en formato papel, soporte informático o a través de Internet, de acuerdo con las normas de cumplimentación a las que habrán de adecuarse las notificaciones de ficheros incluidas en el anexo II de esta Resolución.

Cuarto.

Mediante el formulario electrónico NOTA se podrán presentar notificaciones a través de Internet firmadas mediante certificado digital de firma reconocido de acuerdo con lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica. La relación actualizada de certificados de firma válidos para presentar notificaciones en el registro Telemático de la AEPD se podrá consultar en la página web de la AEPD.

Quinto.

Cuando la notificación se envíe a través de Internet sin certificado de firma electrónica reconocido, sólo se considerará recibida la notificación efectuada desde la fecha en la que tenga entrada en la Agencia Española de Protección de Datos la hoja de solicitud firmada de forma manual. En todo caso, carecerán de efecto alguno las notificaciones si la hoja de solicitud, debidamente cumplimentada y firmada, no hubiera sido presentada en la Agencia Española de Protección de Datos o en alguno de los Registros y oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992, en el plazo de los diez días siguientes al envío de la notificación a través de Internet sin certificado de firma electrónica reconocido.

Sexto.

Podrán desarrollarse utilidades informáticas para la remisión de notificaciones al Registro General de Protección de Datos, debiendo las mismas atenerse al formato XML y a las normas de cumplimentación aprobadas en el anexo II. Las especificaciones técnicas para la remisión de estos ficheros podrán consultarse en la página web de la AEPD.

Estos mensajes en formato XML pueden ser presentados con y sin certificado electrónico de firma reconocido. En el caso de que se presenten firmados electrónicamente deberán utilizar el estándar de firma Xml Digital Signature, cuya especificación de sintaxis y procesamiento se encuentra en http://www.w3.org/2000/09/xmldsig#. En este caso, una vez enviadas las notificaciones al Registro Telemático de la AEPD, éste devolverá un mensaje confirmando la recepción del envío incluyendo, a su vez, los datos necesarios para que el programa desarrollado por terceros configure el acuse de recibo de acuerdo con el formato que figura en el anexo III.

En el caso de que las notificaciones se presenten mediante formato XML sin certificado de firma electrónica, el servidor web de la AEPD devolverá un mensaje confirmando la recepción del envío e incluyendo, a su vez, los datos necesarios para que el programa desarrollado por terceros configure la Hoja de solicitud de acuerdo con el formato que figura en el anexo III. En todo caso, carecerán de efecto alguno las notificaciones si la hoja de solicitud, debidamente cumplimentada y firmada, no hubiera sido presentada en la Agencia Española de Protección de Datos o en alguno de los Registros y oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992, en el plazo de los diez días siguientes al envío de las notificaciones a través de Internet mediante formato XML sin certificado de firma electrónica reconocido.

Séptimo.

Todas las recepciones de soportes informáticos y telemáticos serán provisionales, a resultas de su proceso y comprobación. Cuando no se ajusten al diseño y demás especificaciones establecidas en la presente Resolución, se requerirá al declarante para que subsane la notificación en el plazo de 10 días establecido en el artículo 71.1 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Si transcurrido dicho plazo no se hubiera recibido su notificación, se le tendrá por desistido de su petición, procediéndose sin más trámite al archivo de su solicitud.

Octavo.

Las versiones actualizadas de los formularios electrónicos de notificaciones Telemáticas a la AEPD, así como los anexos y requerimientos técnicos a los que se hace referencia en la presente Resolución estarán disponibles en la página web de la Agencia Española de Protección de Datos.

Noveno.

En tanto no se dicte una Resolución de la Agencia Española de Protección de Datos en que se señale expresamente lo contrario continuarán siendo válidas las notificaciones cumplimentadas con arreglo al programa de generación de notificaciones de ficheros de titularidad pública y privada aprobado mediante Resolución de la Agencia Española de Protección de Datos 30 de mayo de 2000.

Las notificaciones efectuadas mediante los formularios de notificación en soporte papel de ficheros de titularidad pública y privada, aprobados mediante Resolución de 30 de mayo de 2000, continuarán siendo válidas siempre que las mismas tengan entrada en la Agencia Española de Protección de Datos con anterioridad al 1 de diciembre de 2006.

Décimo.

El Registro General de Protección de Datos adecuará de oficio las notificaciones efectuadas conforme a los dos últimos párrafos del apartado anterior a los nuevos modelos aprobados mediante la presente Resolución.

Del mismo modo, procederá a la adecuación a los nuevos modelos de las notificaciones referidas a los ficheros inscritos en el Registro en la fecha de entrada en vigor de la presente Resolución.

Undécimo.

La presente Resolución entrará en vigor el día 1 de septiembre de 2006.

ANEXOS

Téngase en cuenta que se han omitido los Anexos que contienen los formularios que pueden consultarse en la página web de la Agencia Española de Protección de Datos www.agpd.es.

§ 17

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras

Agencia Española de Protección de Datos
«BOE» núm. 296, de 12 de diciembre de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-21648

El incremento que últimamente están experimentando las instalaciones de sistemas de cámaras y videocámaras con fines de vigilancia ha generado numerosas dudas en lo relativo al tratamiento de las imágenes que ello implica. Además es un sector que ofrece múltiples medios de tratar datos personales como pueden ser los circuitos cerrados de televisión, grabación por dispositivos «webcam», digitalización de imágenes o instalación de cámaras en el lugar de trabajo. Precisamente la última Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Londres los pasados días 1 a 3 de noviembre de este año, ha girado en torno a la necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos. Todo esto hace necesario que, en ejercicio de la competencia que le atribuye el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la Agencia Española de Protección de Datos dicte una Instrucción para adecuar los tratamientos de imágenes con fines de vigilancia a los principios de dicha Ley Orgánica y garantizar los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos.

El marco en que se mueve la presente Instrucción es claro. La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático.

Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999 y el artículo 1.4 del Real Decreto 1332/1994 de 20 de junio, que considera como dato de carácter personal la información gráfica o fotográfica.

En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

En cuanto a la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

Asimismo la proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, tales como la instalación de sistemas de vigilancia en espacios comunes, o aseos del lugar de trabajo. Por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona.

Se excluyen de la presente Instrucción los datos personales grabados para uso o finalidad doméstica de conformidad con lo establecido en el artículo 2 a) de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, si bien en el sentido estricto señalado por el Tribunal de Justicia de las Comunidades Europeas en la Sentencia de 6 de noviembre de 2003, asunto Lindqvist, que al interpretar la excepción prevista en el artículo 3 apartado 2 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, indica que únicamente contempla «las actividades que se inscriben en el marco de la vida privada o familiar de los particulares» y no otras distintas. En la misma línea se pronuncia el Dictamen 4/2004, adoptado por el Grupo de Trabajo creado por el Artículo 29 de la Directiva 95/46/CE, con fecha 25 de noviembre de 2002.

Además, la Instrucción tampoco se aplicará al tratamiento de imágenes cuando éstas se utilizan para el ejercicio de sus funciones por parte de las Fuerzas y Cuerpos de Seguridad, que está cubierto por normas específicas, aunque estos tratamientos también deberán cumplir las garantías establecidas por la Ley Orgánica 15/1999.

Por otro lado, la Instrucción pretende adecuar los tratamientos a los criterios marcados por la jurisprudencia del Tribunal Constitucional al considerar que el tratamiento de datos personales no exige la conservación de los mismos, sino que basta su recogida o grabación. En el mismo sentido se han pronunciado las legislaciones que sobre esta materia han adoptado los distintos Estados miembros de la Unión Europea, cumpliendo así el mandato contenido en la Directiva 95/46/CE.

Por último, las plenas garantías de protección de los datos personales, así como las peculiaridades de su tratamiento exige una regulación concreta evitando la aplicación de un conjunto de reglas abstractas y dispersas. Por ello, a la hora de regular la legitimación del tratamiento de imágenes, la Agencia Española de Protección de Datos, entiende que es requisito esencial la aplicación íntegra del artículo 6.1 y 2 y del artículo 11.1 y 2 de la LOPD, sin perjuicio del estricto cumplimiento de los requisitos que para la instalación de cámaras o videocámaras de vigilancia vengan exigidos por la legislación vigente. Asimismo se regula el contenido del deber de información previsto en el artículo 5 de la misma Ley Orgánica, así como el ejercicio de los derechos a que se refieren los artículos 15 y siguientes de la citada Ley Orgánica. Por descontado, la creación de un fichero de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General.

En su virtud, de conformidad con lo dispuesto en el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, dispongo:

Artículo 1. *Ámbito objetivo.*

1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.

2. El tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad se regirá por las disposiciones sobre la materia.

3. No se considera objeto de regulación de esta Instrucción el tratamiento de imágenes en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar.

Artículo 2. *Legitimación.*

1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.

Artículo 3. *Información.*

Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.

Artículo 4. *Principios de calidad, proporcionalidad y finalidad del tratamiento.*

1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

Artículo 5. *Derechos de las personas.*

1. Para el ejercicio de los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, el/la afectado/a deberá remitir al responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada. El ejercicio de estos derechos se llevará a cabo de conformidad con lo dispuesto en la citada Ley Orgánica y su normativa de desarrollo.

2. El responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.

3. El/la interesado/a al que se deniegue total o parcialmente el ejercicio de los derechos señalados en el párrafo anterior, podrá reclamar su tutela ante el Director de la Agencia Española de Protección de Datos.

Artículo 6. *Cancelación.*

Los datos serán cancelados en el plazo máximo de un mes desde su captación.

Artículo 7. *Notificación de ficheros.*

1. La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

Articulo 8. *Seguridad y Secreto.*

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior.

Disposición transitoria.

Los responsables de ficheros de videovigilancia ya inscritos en el Registro General de la Agencia Española de Protección de Datos deberán adoptar las medidas previstas en el artículo 3, letra a), y en el artículo 4.3 de esta Instrucción en el plazo máximo de tres meses desde su entrada en vigor.

Disposición final.

La presente Instrucción entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

2. El modelo a que se refiere el apartado anterior, está disponible en la página web de la Agencia Española de Protección de Datos, www.agpd.es, de donde podrá ser descargado, especificando los datos del responsable.

§ 18

Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones

Agencia Española de Protección de Datos
«BOE» núm. 4, de 5 de enero de 2005
Última modificación: sin modificaciones
Referencia: BOE-A-2005-186

I

Uno de los objetivos fundamentales de la Agencia Española de Protección de Datos es el de lograr la mayor transparencia en su actividad, para una mejor garantía y tutela del derecho fundamental a la protección de datos de carácter personal, en el marco del proceso de implantación de la sociedad de la información.

Desde su creación, cada año se ha publicado una Memoria de la Agencia Española de Protección de Datos. A través de estas memorias se ha podido tener conocimiento de las actividades desarrolladas por la Agencia, de los procedimientos que se han seguido en la misma y de los criterios con que han sido resueltos. Sin embargo, dado el tiempo que transcurre desde que se dicta una resolución hasta que se publica la Memoria han podido existir desfases en el conocimiento del parecer de la Agencia.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, tras la modificación introducida por el artículo 82.1 de la Ley 62/2003, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, establece en el artículo 37.2 que las resoluciones de la Agencia Española de Protección de Datos, a excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo regulados en el artículo 32 de la citada Ley, se harán públicas, una vez hayan sido notificadas a los interesados, preferentemente a través de medios informáticos o telemáticos.

Con la modificación introducida por la citada Ley 62/2003, la Agencia tiene, por consiguiente, la obligación de hacer públicas sus resoluciones desde el momento en que han sido notificadas a los interesados, lo que sin duda redundará en un mejor conocimiento de sus criterios y una mayor seguridad jurídica en la aplicación de la Ley. Dado que dicha Ley entró en vigor el día 1 de enero de 2004, sus disposiciones en materia de publicidad de las resoluciones de la Agencia Española de Protección de Datos afectarán a todas aquéllas dictadas en procedimientos incoados a partir de dicha fecha, así como a las correspondientes al archivo de actuaciones inspectoras iniciadas desde esa misma fecha.

Con ello, se potencia el conocimiento de los criterios en la aplicación de la normativa sobre protección de datos, se facilita su cumplimiento y se favorece, asimismo, la aplicación de los principios de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

II

El artículo 37.1 c) de la Ley Orgánica 15/1999 atribuye a la Agencia Española de Protección de Datos la función de «dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley». La potestad normativa de la Agencia ha sido expresamente reconocida por el Tribunal Constitucional, en su Sentencia 290/2000, de 30 de noviembre.

En ejercicio de dicha potestad se dicta la presente Instrucción, cuyo objeto es establecer los términos en los que la Agencia Española de Protección de Datos va a realizar la publicación de las resoluciones a las que hace referencia el artículo 37.2 de la Ley Orgánica 15/1999.

Con dicho objeto, se establece la forma y los plazos en que se realizará la publicación de las indicadas resoluciones y, se prevé que, en todo caso, a fin de salvaguardar el derecho fundamental a la protección de datos de carácter personal, será necesario proceder a la disociación de dichos datos.

Asimismo, se dispone que en las resoluciones a las que se refiere el artículo 37.2 de la Ley Orgánica 15/1999, la Agencia hará constar, de forma expresa, que procederá a su publicación.

En su virtud, de conformidad con lo dispuesto en el artículo 37.1 c) de la Ley Orgánica 15/1999 y de acuerdo con el Consejo Consultivo de la Agencia Española de Protección de Datos,

DISPONGO:

Norma primera.

De conformidad con lo establecido en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, según la redacción dada por el artículo 82.1 de la Ley 62/2003, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, la Agencia Española de Protección de Datos hará públicas sus resoluciones, a excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo regulados en el artículo 32 de la Ley Orgánica 15/1999, siempre que se refieran a procedimientos que se hubieran iniciado a partir del 1 de enero de 2004, o correspondan al archivo de actuaciones inspectoras incoadas desde dicha fecha.

Norma segunda.

La publicación de estas resoluciones se realizará en la página web de la Agencia Española de Protección de Datos, en el plazo de un mes a contar desde el día siguiente al de su notificación a los interesados.

Norma tercera.

En las resoluciones a las que se refiere la norma primera se hará constar expresamente que la Agencia va a proceder a su publicación en los términos establecidos en la presente Instrucción.

Norma cuarta.

La publicación de las resoluciones a que se refiere la presente Instrucción se realizará previa disociación de los datos de carácter personal a los que se refiere el artículo 3 a) de la Ley Orgánica 15/1999.

La publicación de dichas resoluciones no contendrá, en ningún caso, los datos referentes al domicilio de las personas jurídico privadas, empresarios individuales o profesionales afectados por la resolución.

Norma quinta.

Las resoluciones correspondientes a los procedimientos y actuaciones de inspección que se mencionan en la norma primera iniciados a partir del 1 de enero de 2004 y que hayan sido notificadas antes de la fecha de entrada en vigor de la presente Instrucción, se publicarán en el plazo de tres meses a partir de la misma.

Norma sexta.

La presente Instrucción entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

§ 19

Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos

Agencia de Protección de Datos
«BOE» núm. 301, de 16 de diciembre de 2000
Última modificación: sin modificaciones
Referencia: BOE-A-2000-22726

El régimen del movimiento internacional de datos de carácter personal ha sido, desde la aprobación de la derogada Ley Orgánica 5/1992, de 29 de octubre, de regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), una de las cuestiones que ha suscitado un mayor número de dudas por parte de los responsables de los ficheros y la sociedad en general.

El motivo de estas dudas probablemente se encuentre en el hecho de que las normas reguladoras en esta materia contenidas en la Ley y sus normas de desarrollo hayan debido adaptarse a las incluidas en los artículos 25 y 26 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como por las Decisiones que, en cumplimiento de los citados preceptos se adopten por la Comisión de las Comunidades Europeas.

La actuación de la Agencia de Protección de Datos en sus casi siete años de existencia ha generado una abundante casuística relacionada con las transferencias internacionales de datos de carácter personal que hasta la fecha no venía recogida sistemáticamente en ningún texto.

Por otra parte, el artículo 37 c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, consagra la competencia de la Agencia de Protección de Datos para «dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley».

En uso de esta facultad, la presente Instrucción tiene por objeto señalar los criterios orientativos seguidos por la Agencia de Protección de Datos en relación con aquellos tratamientos que supongan una transferencia internacional de datos, poniendo de manifiesto el procedimiento que, en uso de las competencias que la Ley le atribuye, se sigue por la Agencia en cada caso concreto.

Por tanto no es finalidad de esta Instrucción efectuar innovación alguna dentro de la normativa reguladora de la protección de datos de carácter personal sino, simplemente, aclarar y facilitar a todos los interesados en un único texto, el procedimiento seguido por la Agencia para dar cumplimiento a las previsiones contenidas en la diversidad de normas que se refieren al movimiento internacional de datos.

II

Los artículos 33 y 34 de la Ley Orgánica 15/1999 establecen el régimen al que habrán de someterse los movimientos internacionales de datos. Estos preceptos, sin modificar el criterio general que habrá de regir las transferencias, esto es, la exigencia de autorización del Director de la Agencia de Protección de Datos, vienen a adecuar el régimen de excepciones a dicha autorización, añadiendo a los ya contemplados en la LORTAD otros deducidos de lo dispuesto en los artículos 25 y 26 de la Directiva 95/46/CE. En particular, el artículo 34 k) de la Ley Orgánica 15/1999 exceptúa del régimen general de autorización el supuesto en que «la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado».

En este sentido, deben tenerse en cuenta las recintes Decisiones de la Comisión de las Comunidades Europeas, números 2000/518/CE, 2000/519/CE y 2000/520/CE, de 26 de julio (publicadas en el Diario Oficial de las Comunidades Europeas de 25 de agosto de 2000), que consideraron adecuado el nivel de protección de datos personales en Suiza, Hungría, así como «el conferido por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos».

El régimen regulador del movimiento internacional de datos se encuentra, en todo caso, gobernado por el principio general, contenido en el artículo 25.1 de la Directiva, de que la transferencia a empresas o Administraciones ubicadas en el territorio de terceros Estados deberá entenderse «sin perjuicio del cumplimiento de las disposiciones de derecho nacional adoptadas con arreglo a las disposiciones de la presente Directiva». En este mismo sentido se pronuncian las Decisiones de la Comisión de las Comunidades Europeas a las que acabamos de hacer referencia en su artículo 2.

III

A la vista de todo ello, la presente Instrucción se divide en dos Secciones:

La primera de ellas establece criterios predicables de la totalidad de las transferencias internacionales de datos, indicando los conceptos generales que han de ser tenidos en cuenta para el cumplimiento de lo indicado en la Ley. Se recuerda además en esta Sección el principio general referente al necesario cumplimiento de la Ley Orgánica 15/1999 por parte de aquellas personas o entidades que pretendan efectuar una transferencia internacional de datos. Por último, se señala el procedimiento que las normas vigentes prevén para la notificación de dicha transferencia a esta Agencia de Protección de Datos.

La segunda Sección se refiere a supuestos concretos de transferencias. En particular, se contemplan tres supuestos específicos, dos atendiendo al país al que los datos se destinen y uno en función de la finalidad última que motiva la transferencia.

Así, la norma cuarta se refiere a aquellos países no comunitarios respecto de los que se haya declarado la existencia de un nivel de protección adecuado, con especial referencia al supuesto contemplado por la Decisión 2000/520/CE, de la Comisión de las Comunidades Europeas, a la que ya se ha hecho referencia.

La norma quinta toma en consideración la solución contractual en el supuesto de transferencias que exijan la autorización del Director de la Agencia de Protección de Datos, conforme a lo dispuesto en el artículo 33 de la Ley Orgánica 15/1999, indicando aquellos extremos que la Agencia ha venido considerando necesarios para que se entienda que la transferencia ofrece un adecuado nivel de garantía. La solución contractual ha sido considerada por el Parlamento Europeo, en su informe de 11 de julio de 2000, el instrumento más eficaz para garantizar que la transferencia de datos ofrece las garantías adecuadas. También el Documento del Grupo de Trabajo de Protección de Datos, creado por el artículo 29 de la Directiva Comunitaria, referente a los criterios de interpretación del régimen de transferencias internacionales, de 24 de julio de 1998, contiene previsiones específicas referidas a esta solución contractual.

Por último, la norma sexta se refiere a aquellos casos en que, con independencia del Estado al que se destinen los datos, la transferencia trae causa de la contratación de un

servicio de tratamiento de datos por cuenta del responsable del fichero, transmitiéndose los datos a quien la Ley 15/1999 define como «encargado del tratamiento». En este caso deberá existir, en virtud de lo dispuesto en el artículo 12 de la Ley, y sin perjuicio del cumplimiento de los demás requisitos a los que se refiere la presente Instrucción, un contrato entre las entidades transmitente y destinataria de los datos.

En su virtud, en uso de las facultades que le atribuye el artículo 37 c) de la Ley Orgánica 15/1999, esta Agencia ha dispuesto:

Sección I. Disposiciones generales

Norma primera. *Ámbito de aplicación.*

La presente Instrucción será de aplicación a cualquier supuesto de transferencia internacional de datos de carácter personal.

A tal efecto, se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero.

A los efectos de esta instrucción, se entiende por transmitente la persona física o jurídica, pública o privada, responsable del fichero o tratamiento de los datos de carácter personal que son objeto de transferencia internacional, y por destinatario la persona física o jurídica, pública o privada, situada fuera del territorio español que recibe los datos transferidos.

Norma segunda. *Cumplimiento de las disposiciones de la Ley Orgánica 15/1999.*

La transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia de Protección de Datos la competencia para verificar su cumplimiento.

En todo caso, de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 15/1999, cualquier responsable de un fichero o tratamiento que se proponga transferir datos de carácter personal fuera del territorio español deberá haber informado a los afectados de quiénes serán destinatarios de los datos, así como de la finalidad que justifica la transferencia internacional y el uso de los datos que podrá hacer el destinatario.

El deber de información al que se refiere el párrafo anterior no será de aplicación cuando la transferencia tenga por objeto la prestación de un servicio al responsable del fichero, en los términos establecidos por el artículo 12 de la Ley Orgánica 15/1999.

Norma tercera. *Notificación de las transferencias previstas al Registro General de Protección de Datos.*

1. De conformidad con el artículo 26.2 de la Ley Orgánica 15/1999 cualquier persona o entidad que pretenda efectuar una transferencia internacional de datos deberá hacerlo constar expresamente al proceder a la notificación del fichero al Registro General de Protección de Datos.

La notificación de la transferencia se efectuará en los términos que se contengan en el modelo normalizado aprobado a tal efecto por el Director de la Agencia de Protección de Datos, con expresa indicación del país al que se pretende efectuar la transferencia y de los motivos que, en su caso, la habilitan, conforme a lo dispuesto en el artículo 34 de la citada Ley Orgánica, para no recabar la autorización expresa del Director de la Agencia de Protección de Datos.

En caso de que la transferencia internacional se refiera a datos contenidos en un fichero ya inscrito en el Registro General de Protección de Datos, no constando la transferencia en la inscripción, el responsable del fichero deberá solicitar una modificación de la misma, notificando los extremos a los que se refiere el párrafo anterior.

Si se tratara de ficheros de titularidad pública, la transferencia deberá estar prevista en la norma de creación o modificación del fichero.

2. Recibida la notificación, la Agencia de Protección de Datos podrá requerir al responsable del fichero para que en el plazo de diez días aporte la documentación necesaria para completar la información relativa a la trasferencia internacional contenida en aquélla, así como la identidad del receptor de la misma.

A tal efecto, podrá solicitarse del responsable del fichero o tratamiento que aporte la documentación que acredite el cumplimiento de la obligación a la que se refiere la norma segunda de esta Instrucción. En particular, si el responsable invocase la existencia de consentimiento del afectado a la transferencia, podrá solicitarse que acredite la prestación de ese consentimiento. Del mismo modo podrá exigirse que se acredite la existencia de una relación contractual con el afectado que motive la transferencia, si aquélla hubiera sido alegada.

Igualmente, se podrá solicitar del responsable del fichero que acredite los extremos a los que se refiere la Sección Segunda de la presente Instrucción.

Al requerirse la información a la que se refiere este apartado se indicará al responsable del fichero que, en caso de no ser aquélla aportada en el plazo de diez días, se le tendrá por desistido de su petición de inscripción o modificación, archivándose ésta.

3. Si con la documentación aportada no se acreditara el cumplimiento de los requisitos contenidos en la Ley Orgánica 15/1999, el Director de lasAgencia de Protección de Datos, en ejercicio de las competencias que le atribuye dicha Ley Orgánica, denegará la Inscripción o su modificación.

4. Contra las resoluciones del Director de la Agencia de Protección de Datos relativas a la inscripción o, en su caso, a la modificación de un fichero, cabrá interponer potestativamente recurso previo de reposición o recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

Sección II. Disposiciones aplicables a transferencias concretas

Norma cuarta. *Transferencias al territorio de Estados que otorguen un nivel adecuado de protección.*

1. Cuando la transferencia internacional tenga por destinatario una persona o entidad, pública o privada, situada en el territorio de un Estado no miembro de la Unión Europea, respecto del que se haya declarado la existencia de un nivel adecuado de protección o que sea miembro del Espacio Económico Europeo, se podrá requerir al responsable del fichero la aportación de la documentación a la que se refiere el apartado segundo de la norma tercera de esta Instrucción.

2. Sin perjuicio de lo dispuesto en la norma segunda, el Director de la Agencia de Protección de Datos, en uso de la potestad que le otorga el artículo 37 f) de la Ley Orgánica 15/1999, podrá acordar, previa audiencia del transmitente, la suspensión temporal de la transferencia de datos hacia un receptor ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes, previstas en las Decisiones de la Comisión de las Comunidades Europeas:

a) Que las Autoridades de Protección de Datos del Estado destinatario o cualquier otra, en caso de no existir las primeras, resuelvan que el destinatario ha vulnerado las normas de protección de datos de su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad destinataria de la transferencia y que las autoridades competentes en el Estado en que se encuentre el destinatario no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

En estos casos, la decisión del Director de la Agencia de Protección de Datos será notificada a la Comisión de las Comunidades Europeas.

3. Si la transferencia se funda en lo establecido en la Decisión 2000/520/CE de la Comisión de las Comunidades Europeas, «sobre la adecuación de la protección conferida

por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos», quien pretenda efectuar la transferencia deberá acreditar que el destinatario se encuentra entre las entidades que se han adherido a los principios, así como que el mismo se encuentra sujeto a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el Anexo VII de la citada Decisión.

4. Lo indicado en el apartado anterior será de aplicación a todos los supuestos en que el nivel de protección adecuado se declare por la Comisión de las Comunidades Europeas en relación con un sistema de autorregulación o de condiciones similares a las contenidas en la Decisión 2000/520/CE.

5. Contra las resoluciones del Director de la Agencia de Protección de Datos a las que se refiere esta norma cabrá interponer potestativamente recurso previo de reposición o recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

Norma quinta. *Transferencias al territorio de otros Estados.*

1. Cuando la transferencia internacional tenga por destinatario una persona física o jurídica, pública o privada, situada en el territorio de un Estado no miembro de la Unión Europea, respecto del que no se haya declarado por la Comisión de las Comunidades Europeas la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo y el transmitente se funde en alguno de los supuestos comprendidos en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, la Agencia de Protección de Datos podrá requerir al responsable del fichero para que aporte la documentación que justifique su alegación.

2. En caso de que la transferencia no se fundamente en alguno de los supuestos a los que se refiere el apartado anterior, o cuando esta circunstancia no haya quedado debidamente acreditada, será necesario recabar la autorización del Director de la Agencia de Protección de Datos, conforme a lo dispuesto en el artículo 33 de la Ley Orgánica 15/1999.

Sin perjuicio de lo establecido en el apartado 7 de esta norma, dicha autorización será otorgada en caso de que el responsable del fichero aporte un contrato escrito, celebrado entre el transmitente y el destinatario, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

El citado contrato deberá contener, al menos, las siguientes menciones:

a) La identificación del transmitente y el destinatario de los datos.

b) La indicación de la finalidad que justifica la transferencia internacional, así como de los datos que son objeto de la transferencia.

c) El compromiso del transmitente de que la recogida y tratamiento de los datos en territorio español respeta íntegramente las normas contenidas en la Ley Orgánica 15/1999 y que el fichero en que se encuentran los datos objeto de la transferencia está inscrito en el Registro General de Protección de Datos o se ha solicitado su inscripción.

d) El compromiso del destinatario de que los datos recibidos serán tratados exclusivamente para la finalidad que motiva la transferencia, así como que procederá a su tratamiento de acuerdo con las normas de protección de datos del derecho español. Asimismo, el destinatario deberá comprometerse a no comunicar los datos a ningún tercero en tanto no haya sido recabado el consentimiento del afectado para ello.

e) Que el destinatario adoptará las medidas de seguridad requeridas por la normativa de protección de datos de carácter personal vigente en España.

f) Que el transmitente y el destinatario responderán solidariamente frente a los particulares, a la Agencia de Protección de Datos y a los Órganos Jurisdiccionales españoles por los eventuales incumplimientos del contrato en que pudiera incurrir el receptor, cuando los mismos sean constitutivos de infracción de lo dispuesto en la Ley Orgánica 15/1999 o produzcan un perjuicio a los afectados.

g) Que se indemnizará al afectado que resulte perjudicado como consecuencia del tratamiento efectuado por el destinatario, según el régimen de responsabilidad al que se refiere el apartado anterior.

h) La garantía de que el afectado podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición, tanto ante el transmitente como ante el destinatario de los datos. Asimismo, deberá indicarse que el interesado podrá recabar la tutela de la Agencia de Protección de Datos en los supuestos previstos en la Ley Orgánica 15/1999 en caso de que sus derechos no sean atendidos.

i) El compromiso del destinatario de los datos de autorizar el acceso al establecimiento donde se estén tratando los mismos, así como a la documentación y a los equipos físicos y lógicos, de representantes de la Agencia de Protección de Datos o de la entidad independiente en quien ésta delegue, cuando la Agencia lo requiera con el fin de verificar el cumplimiento de las obligaciones derivadas del contrato.

j) La obligación de que, una vez extinguida la relación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transferencia.

k) Que los afectados podrán exigir el cumplimiento de lo estipulado en el contrato en todas aquellas cuestiones en que el mismo les resulte beneficioso.

3. Remitido el contrato, la Agencia de Protección de Datos podrá solicitar que en el mismo se introduzcan las modificaciones necesarias para garantizar el cumplimiento de los requisitos a los que se refieren los dos apartados anteriores, concediendo a tal efecto un plazo de diez días.

4. Transcurrido ese plazo sin que el contrato cumpla los requisitos previstos en los apartados 2 y 3 de esta norma, el Director de la Agencia de Protección de Datos denegará la transferencia solicitada.

5. Cuando el Director de la Agencia de Protección de Datos autorice la transferencia ordenará su inscripción en el Registro General de Protección de Datos y procederá a su comunicación a la Comisión de las Comunidades Europeas.

6. Surtirán el mismo efecto jurídico los contratos que pudieran celebrarse en el futuro al amparo de lo que, en su caso, dispongan las Decisiones de la Comisión de las Comunidades Europeas que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE, siempre que se acredite su íntegro cumplimiento.

7. Sin perjuicio de lo dispuesto en los apartados anteriores de esta norma y en la norma segunda, el Director de la Agencia de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37 f) de la Ley Orgánica 15/1999, suspender temporalmente, previa audiencia del transmitente, la transferencia, cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el destinatario.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

Las resoluciones del Director de la Agencia de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

8. Contra las resoluciones del Director de la Agencia de Protección de Datos cabrá interponer potestativamente recurso previo de reposición o recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

Norma sexta. *Especialidades en las transferencias que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero.*

1. Cuando la transferencia internacional de datos tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero, la realización del tratamiento deberá estar regulada en un contrato, en que deberá hacerse constar la responsabilidad directa de la transmitente como consecuencia de cualquier incumplimiento de la Ley en que incurriera el destinatario.

El contrato, que deberá constar por escrito, establecerá expresamente que el destinatario únicamente tratará los datos conforme a las instrucciones del transmitente, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato y que adoptará las medidas de seguridad exigibles al transmitente conforme a las normas de protección de datos del Derecho español.

Además, deberá indicarse que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento

2. La receptora no podrá comunicar los datos, ni siquiera para su conservación, a otras personas.

En consecuencia, si la transmitente deseara que por parte de varias entidades distintas, situadas fuera del territorio español, se presten servicios de tratamiento, en los términos a que se refiere el artículo 12 de la Ley Orgánica 15/1999, deberá contratar dichos servicios con cada una de las entidades, no siendo posible que la destinataria subcontrate esta segunda actividad con otra empresa, a menos que actúe en nombre y por cuenta del responsable del fichero.

3. En caso de que la transferencia se dirija a un destinatario situado en un Estado no miembro de la Unión Europea respecto del que no se haya declarado la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo, en el contrato deberán constar cautelas semejantes a las indicadas en la norma quinta en lo referente al régimen sancionador y de indemnización a los interesados, así como en lo relativo a las potestades de la Agencia de Protección de Datos, para el caso en que la destinataria emplee los datos para otra finalidad distinta de la que motivó la transferencia, los comunique o los utilice incumpliendo las estipulaciones del contrato.

§ 20

Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo

Agencia de Protección de Datos
«BOE» núm. 62, de 12 de marzo de 1996
Última modificación: sin modificaciones
Referencia: BOE-A-1996-5698

La necesidad de establecer la forma de llevar los ficheros automatizados utilizados para controlar la entrada en casinos y salas de bingo obliga a precisar una serie de criterios interpretativos que faciliten la aplicación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, con mayor razón desde la aprobación de la Directiva europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En concreto, es necesario regular el cumplimiento del deber de información al ciudadano en la recogida de datos personales, el consentimiento en la cesión de los datos así recabados en los supuestos en que la misma no debe efectuarse por causas legales, así como el plazo en que los datos deben ser cancelados por haber dejado de ser necesarios o pertinentes para los fines para los que se recabaron.

La Instrucción solamente se refiere al ámbito competencial propio de la Ley reguladora del tratamiento automatizado de datos personales y se dicta de conformidad con lo dispuesto en el artículo 36.c) de la misma que atribuye a la Agencia de Protección de Datos competencias en esta materia.

Norma primera. *Ámbito de aplicación.*

1. La presente Instrucción regula los datos de carácter personal tratados de forma automatizada que son recabados con la finalidad de controlar el acceso por las sociedades explotadoras de casinos de juego o por cualquier empresa titular de una sala de bingo.

2. A tales efectos, tendrá la consideración de dato personal cualquier información concerniente a personas físicas identificadas o identificables, debiendo entenderse comprendidos dentro de la misma el sonido y la imagen.

Norma segunda. *Responsable del fichero.*

1. Tendrá la consideración de responsable del fichero la sociedad explotadora del casino de juego o la empresa titular de la sala de bingo.

2. El responsable del fichero asumirá el cumplimiento de todas las obligaciones establecidas en la Ley Orgánica 5/1992 y, entre ellas, la de la inscripción del fichero en el Registro General de Protección de Datos.

Norma tercera. *Recogida de datos.*

1. La recogida de datos efectuada para el cumplimiento de los fines a los que se refiere la presente Instrucción deberá realizarse de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 5/1992, y, en concreto, deberá informarse de la existencia de un fichero automatizado, de la finalidad de la recogida de datos, de los destinatarios de la información, del carácter obligatorio de su respuesta, de las consecuencias de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación y de la identidad y dirección del responsable del fichero.

2. No podrán recogerse más datos personales que aquellos estrictamente necesarios para controlar el acceso, quedando, en todo caso, limitados a los que aparecen en el documento identificador exigido para la entrada.

Norma cuarta. *Utilización de los datos.*

Los datos personales así obtenidos no podrán ser utilizados para otros fines. Tampoco podrán ser objeto de cesión los datos así recabados fuera de los casos expresamente establecidos en la ley, salvo consentimiento del afectado.

Norma quinta. *Cancelación de los datos.*

Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de seis meses, contado a partir de la fecha del último acceso.

Norma sexta. *Medidas de seguridad.*

El responsable del fichero garantizará la adopción de las medidas técnicas y organizativas necesarias para la seguridad de los datos y que impidan el acceso no autorizado a los ficheros creados para dichos fines.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor a partir de los tres meses de su publicación en el «Boletín Oficial del Estado».

§ 21

Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación

Agencia de Protección de Datos
«BOE» núm. 25, de 29 de enero de 1998
Última modificación: sin modificaciones
Referencia: BOE-A-1998-1943

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, dedica los artículos 14 y siguientes a los derechos de acceso, rectificación y cancelación de los datos de carácter personal contenidos en ficheros automatizados. Dichos derechos se configuran como uno de los ejes fundamentales sobre los que se articula la protección del honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, en desarrollo de lo dispuesto en el artículo 18.4 de la Constitución Española.

El ejercicio de los derechos de acceso, rectificación y cancelación aparece regulado no sólo en la Ley Orgánica 5/1992, sino también en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos procedimentales de la citada Ley.

Al amparo de lo dispuesto en el artículo 36.c) de la Ley Orgánica 5/1992 que atribuye al Director de la Agencia la función de «dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la presente Ley», se ha elaborado la presente Instrucción.

Esta Instrucción tiene por objeto aclarar las disposiciones relativas a los derechos de acceso, rectificación y cancelación, ya que las actuaciones practicadas por esta Agencia han puesto de manifiesto que en su aplicación se presentan problemas interpretativos y que es necesario precisar el ejercicio de estos derechos en relación con algunos ficheros que presentan características especiales. Para ello, la Instrucción recoge la regulación de dichos derechos de acuerdo con la Ley Orgánica 5/1992 y el Real Decreto 1332/1994, de 20 de junio, y realiza una interpretación unitaria de los preceptos teniendo en cuenta la totalidad de principios legales.

En las normas primera, segunda y tercera se detallan los requisitos que deben cumplirse en el ejercicio de los derechos de acceso, rectificación y cancelación con carácter general. Sin embargo, las particularidades que presentan los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito y los ficheros con fines de publicidad exigen tratarlos de un modo especial en las normas cuarta y quinta, respectivamente.

Norma primera. *Requisitos generales.*

1. Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero por lo que será necesario que el afectado acredite su identidad frente

a dicho responsable. Estos derechos se ejercerán sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el Real Decreto 1332/1994, de 20 de junio.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que el representante legal acredite tal condición.

2. La Ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

3. El ejercicio de los derechos deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero, que contendrá:

Nombre, apellidos del interesado y fotocopia del documento nacional de identidad del interesado y, en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del documento nacional de identidad podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.

Petición en que se concreta la solicitud.

Domicilio a efectos de notificaciones, fecha y firma del solicitante.

Documentos acreditativos de la petición que formula, en su caso.

El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

4. El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.

En el caso de que la solicitud no reúna los requisitos especificados en el apartado tercero, el responsable del fichero deberá solicitar la subsanación de los mismos.

5. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

Norma segunda. *Derecho de acceso.*

1. El afectado tiene derecho a solicitar y obtener información de sus datos de carácter personal incluidos en ficheros automatizados.

2. Al ejercitar el derecho de acceso, el afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:

a) Visualización en pantalla.

b) Escrito, copia o fotocopia remitida por correo.

c) Telecopia.

d) Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

3. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

4. Si la resolución fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquélla.

5. El responsable del fichero podrá denegar el acceso a los datos de carácter personal cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y no se acredite un interés legítimo al efecto, así como cuando la solicitud sea formulada por persona distinta del afectado.

Tratándose de ficheros de titularidad pública se podrá denegar el acceso en los supuestos de los artículos 21.1 y 21.2 de la Ley Orgánica 5/1992, en los que se establecen

excepciones relativas a los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado y a los ficheros de la Hacienda Pública y del artículo 22 de la Ley Orgánica 5/1992.

6. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, previa transcripción en claro de los datos del fichero, en su caso, y comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas identificando la información que proviene de cada una de ellas.

Norma tercera. *Derechos de rectificación y cancelación.*

1. Si los datos de carácter personal del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, la cancelación de los mismos.

2. Los derechos de rectificación y cancelación se harán efectivos por el responsable del fichero dentro de los cinco días siguientes al de la recepción de la solicitud. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

3. La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado.

4. En la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda, o si, por el contrario, se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

5. La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

6. Si solicitada la rectificación o cancelación, el responsable del fichero considera que no procede atender la solicitud del afectado, se lo comunicará motivadamente dentro del plazo de los cinco días siguientes al de la recepción de la misma, a fin de que por éste se pueda hacer uso de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.

7. Transcurrido el plazo de cinco días sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda.

8. La cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas.

9. En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

Norma cuarta. *Ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito.*

1. El ejercicio de los derechos de acceso, rectificación y cancelación en el caso de los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito se rige por las normas anteriores de la presente Instrucción, sin perjuicio de lo señalado en los apartados siguientes.

2. El responsable de un fichero de prestación de servicios de solvencia patrimonial y crédito con datos obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento, estará obligado a satisfacer, en cualquier caso, los derechos de acceso, rectificación y cancelación. Las personas y entidades a las

que se presta el servicio únicamente estarán obligadas a comunicar al afectado aquellos datos relativos al mismo a los que ellas tengan acceso y a comunicar la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

3. El responsable del fichero común en el que se traten automatizadamente datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés, ante una solicitud de ejercicio del derecho de acceso, deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero. Cualquier otra entidad participante en el sistema, ante tal solicitud, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad del responsable del fichero común para que pueda completar el ejercicio de su derecho de acceso.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige al responsable del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de cinco días, procederá a la rectificación o cancelación cautelar de los mismos.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige a cualquier otra entidad participante en el sistema y hace referencia a datos que dicha entidad haya facilitado al fichero común, procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al responsable del fichero común en el plazo de cinco días. Si la solicitud hace referencia a datos que la entidad no hubiera facilitado al fichero común, dicha entidad informará al afectado sobre este hecho, proporcionándole, además, la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

4. En los ficheros de prestación de servicios de información de solvencia patrimonial y crédito, cualquiera que sea el origen de los datos, cuando el afectado lo solicite el responsable del fichero común deberá cumplir la obligación establecida en el artículo 28.2 de la Ley Orgánica 5/1992 de facilitar, las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

Norma quinta. *Ficheros con fines de publicidad.*

1. El responsable del fichero que presta el servicio de publicidad estará obligado a satisfacer los derechos de acceso, rectificación y cancelación. La entidad beneficiaria de la publicidad estará obligada a indicar al afectado la identidad del responsable del fichero del que provienen los datos. A tal efecto, se entenderá suficiente que dicha información se haga constar en la campaña publicitaria.

2. Cuando el interesado manifieste su deseo de no recibir publicidad, y no ejerza expresamente el derecho de cancelación, el responsable del fichero podrá conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Disposición final única.

La presente Instrucción entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

§ 22

Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios

Agencia de Protección de Datos
«BOE» núm. 62, de 12 de marzo de 1996
Última modificación: sin modificaciones
Referencia: BOE-A-1996-5697

La necesidad de regular los ficheros automatizados establecidos para el control del acceso de las personas a los centros de trabajo o dependencias públicas, a donde se acude con la finalidad de efectuar actividades relacionadas con las propias del centro visitado, plantea problemas relacionados con la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, con mayor razón desde la aprobación de la Directiva europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Estos problemas se concretan en la necesidad de regular los datos constituidos por sonido e imagen, como los de vigilancia por videocámara, y, en general, todos los recopilados en cumplimiento de las funciones de vigilancia, con la prestación del consentimiento necesario para ello, así como el período en que los mismos deban ser conservados y su posterior cancelación por haber dejado de ser necesarios o pertinentes para los fines para los que fueron recabados.

La Instrucción solamente se refiere al ámbito competencial propio de la Ley reguladora del tratamiento automatizado de datos personales y se dicta de conformidad con lo dispuesto en el artículo 36.c) de la misma que atribuye a la Agencia de Protección de Datos competencias en esta materia.

Norma primera. *Ámbito de aplicación.*

1. La presente Instrucción regula los datos de carácter personal tratados de forma automatizada que son recabados por los servicios de seguridad con la finalidad de controlar el acceso a los edificios públicos y privados, así como a establecimientos, espectáculos, certámenes y convenciones.

2. A tales efectos, tendrá la consideración de dato personal cualquier información concerniente a personas físicas identificadas o identificables, debiendo entenderse comprendidos dentro de la misma el sonido y la imagen.

Norma segunda. *Responsable del fichero.*

1. Tendrá la consideración de responsable del fichero la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo por cuya cuenta se efectúe la realización del servicio de seguridad. No obstante lo anterior, mediante el correspondiente

contrato de prestación de servicios de seguridad, podrá tener la consideración de responsable del fichero la empresa que preste los servicios de aquella naturaleza.

2. El responsable del fichero asumirá el cumplimiento de todas las obligaciones establecidas en la Ley Orgánica 5/1992 y, entre ellas, la de la inscripción del fichero en el Registro General de Protección de Datos.

Norma tercera. *Recogida de datos.*

1. La recogida de datos efectuada para el cumplimiento de los fines a los que se refiere la presente Instrucción deberá realizarse de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 5/1992, y, en concreto, deberá informarse de la existencia de un fichero automatizado, de la finalidad de la recogida de los datos, de los destinatarios de la información, del carácter obligatorio de su respuesta, de las consecuencias de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación y de la identidad y dirección del responsable del fichero.

2. Los datos recogidos serán los estrictamente necesarios para cumplir la finalidad de controlar el acceso.

Norma cuarta. *Utilización de los datos.*

Los datos personales así obtenidos no podrán ser utilizados para otros fines. Tampoco podrán ser objeto de cesión los datos así recabados fuera de los casos expresamente establecidos en la ley, salvo consentimiento del afectado.

Norma quinta. *Cancelación de los datos.*

Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados.

Norma sexta. *Medidas de seguridad.*

El responsable del fichero garantizará la adopción de las medidas técnicas y organizativas necesarias para la seguridad de los datos y que impidan el acceso no autorizado a los ficheros creados para dichos fines.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor a partir de los tres meses de su publicación en el «Boletín Oficial del Estado».

§ 23

Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal

Agencia de Protección de Datos
«BOE» núm. 110, de 9 de mayo de 1995
Última modificación: sin modificaciones
Referencia: BOE-A-1995-10931

La concesión de un crédito hipotecario o personal, que suele ir acompañada de un seguro de vida por el importe de aquél y del que se señala como beneficiaria a la entidad de crédito de que se trate por la suma del capital no amortizado, incide sobre un importante número de disposiciones de nuestro ordenamiento jurídico.

Es obvio que la regulación jurídica de alguna de estas materias (Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios; Ley 16/1989, de 17 de julio, de Defensa de la Competencia; Ley 9/1992, de 30 de abril, de Mediación en Seguros Privados), excede de las competencias que tiene atribuidas la Agencia de Protección de Datos. Ahora bien, la precisión de si los datos son o no sensibles, con la incidencia que ello tiene en su recogida, tratamiento y cesión, la determinación del fichero en donde deban ser tratados, la de si es preciso que en esta materia, por tratarse de datos especialmente protegidos, el nivel de protección de los mismos se extienda excepcionalmente a los ficheros manuales o no automatizados, son, entre otras, cuestiones que deben ser fijadas por la Agencia de Protección de Datos.

En consecuencia, en uso de las facultades que tiene conferidas, la Agencia de Protección de Datos ha dispuesto:

Norma primera. *Ámbito de aplicación.*

La presente Instrucción será de aplicación a los datos personales solicitados por las entidades de crédito con motivo de la celebración de un contrato de seguro de vida anejo a la concesión de un crédito hipotecario o personal.

Norma segunda. *De la recogida de los datos.*

1. La obtención de datos personales a efectos de la celebración de un contrato de seguro de vida, anejo a la concesión de un crédito hipotecario o personal, efectuada por las entidades de crédito a través de cuestionarios u otros impresos deberá realizarse, en todo caso, mediante modelos separados para cada uno de los contratos a celebrar. En los formularios cuyo destinatario sean las entidades bancarias no podrán recabarse en ningún caso datos relativos a la salud del solicitante.

2. Cualquiera que sea el modo de llevarse a efecto la recogida de datos de salud necesarios para la celebración del seguro de vida deberá constar expresamente el compromiso de la entidad de crédito de que los datos obtenidos a tal fin solamente serán utilizados por la entidad aseguradora. Las entidades de crédito no podrán incluir los datos de salud en sus ficheros informatizados o en aquéllos en los que almacenen datos de forma convencional.

3. En ningún caso se considerará, por la naturaleza de la información solicitada o por las circunstancias en que se recaba, que se puede prescindir del derecho de la información en la recogida de los datos previstos en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Por tanto, será necesario informar previamente, en los formularios u otros impresos de recogida, de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

e) De la identidad y dirección del responsable del fichero.

4. Cuando la recogida de datos personales a efectos de la celebración de un contrato de seguro de vida, anejo a la concesión de un crédito hipotecario o personal efectuada por las entidades de crédito, se lleve a cabo por procedimientos distintos a los del formulario u otros impresos deberá informarse al afectado de los extremos previstos en el apartado tercero.

Norma tercera. *Consentimiento del afectado y tratamiento de los datos.*

El afectado deberá manifestar su consentimiento por separado para cada uno de los contratos y para el tratamiento distinto de la información que ambos conllevan.

Las entidades de crédito solamente podrán tratar aquellos datos personales, no especialmente protegidos, que sean estrictamente necesarios para relacionar el contrato de préstamo con el contrato de seguro de vida celebrado como consecuencia de aquél o que estén justificados por la intervención de la entidad de crédito como agente o tomador del contrato de seguro.

Norma cuarta. *Cesión de los datos.*

En ningún caso podrá considerarse que la cesión de cualquier clase de datos personales solicitados por la entidad aseguradora a la de crédito, o viceversa, se halla amparada por lo establecido en el artículo 11.2. c), de la Ley Orgánica 5/1992.

Norma transitoria. *Aplicación a contratos celebrados con anterioridad.*

Los datos de salud correspondientes a los contratos de seguro de vida celebrados con anterioridad a la publicación de esta Instrucción, que se encuentren incluidos en ficheros de las entidades de crédito, automatizados o no, deberán ser cancelados en el plazo de un mes, contado a partir de la entrada en vigor de la misma.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado».

§ 24

Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito

Agencia de Protección de Datos
«BOE» núm. 54, de 4 de marzo de 1995
Última modificación: sin modificaciones
Referencia: BOE-A-1995-5746

El artículo 36 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, al definir las funciones de la Agencia de Protección de Datos, incluye en su apartado c) la de dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de dicha Ley. Disposición que tiene su complemento en el artículo 5.c) del Estatuto de la Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo, que señala entre las funciones de la misma la de dictar las instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica.

El artículo 28 de la misma se refiere a la prestación de servicios de información sobre solvencia patrimonial y crédito desde una doble perspectiva. Por un lado, determina que quienes se dediquen a la prestación de servicios sobre la solvencia patrimonial y el crédito sólo podrán tratar automatizadamente datos de carácter personal obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento. Por otro, regula el tratamiento de datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias señalando que podrán tratarse dichos datos siempre que sean «facilitados por el acreedor o por quien actúe por su cuenta o interés».

Los primeros no se apartan de la regulación común que establece la Ley Orgánica; los segundos presentan, por el contrario, un conjunto de especialidades (excepción del principio del consentimiento tanto en la recogida del dato como en su tratamiento), que hacen necesario efectuar una serie de precisiones. Además, dentro de estos últimos, la realidad demuestra que coexisten perfectamente engarzados dos tipos de ficheros: Uno, el propio del acreedor, que se nutre de los datos personales que son consecuencia de las relaciones económicas mantenidas con el afectado, cuya única finalidad es obtener la satisfacción de la obligación dineraria, y otro, un fichero que se podría denominar común que, consolidando todos los datos personales contenidos en aquellos otros ficheros, tiene por finalidad proporcionar información sobre la solvencia de una persona determinada y cuyo responsable, al no ser el acreedor, no tiene competencia para modificar o cancelar los datos inexactos que se encuentran en aquéllos.

En consecuencia, en uso de las facultades que tiene conferidas, la Agencia de Protección de Datos ha dispuesto:

CAPÍTULO I

Calidad de los datos objeto del tratamiento automatizado, forma y veces en que debe efectuarse la notificación y cómputo del plazo al que se refiere el artículo 28.3 de la Ley Orgánica

Norma primera. *Calidad de los datos objeto de tratamiento.*

1. La inclusión de los datos de carácter personal en los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias, a los que se refiere el artículo 28 de la Ley Orgánica 5/1992, deberá efectuarse solamente cuando concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impagada.

b) Requerimiento previo de pago a quien corresponda, en su caso, el cumplimiento de la obligación.

2. No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba documental que aparentemente contradiga alguno de los requisitos anteriores. Tal circunstancia determinará igualmente la desaparición cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero.

3. El acreedor o quien actúe por su cuenta e interés deberá asegurarse que concurren todos los requisitos exigidos en el número 1 de esta norma en el momento de notificar los datos adversos al responsable del fichero común.

4. La comunicación del dato inexistente o inexacto, con el fin de obtener su cancelación o modificación, deberá efectuarse por el acreedor o quien actúe por su cuenta al responsable del fichero común en el mínimo tiempo posible, y en todo caso en una semana. Dicho plazo es independiente del establecido en el artículo 15.2 del Real Decreto 1332/1994, de 20 de junio, y que se aplica al fichero del acreedor.

Norma segunda. *Notificación de la inclusión en el fichero.*

1. La notificación de la inclusión de datos personales en el fichero efectuada con posterioridad a la entrada en vigor de la Ley Orgánica 5/1992 se efectuará en la forma establecida en el artículo 28 de la misma.

2. Cuando se trate de datos personales incorporados al fichero con anterioridad a la entrada en vigor de la Ley Orgánica deberán notificarse al afectado en el menor plazo posible y, en todo caso, dentro del año siguiente contado desde la publicación de la presente Instrucción.

3. La inscripción en el fichero de la obligación incumplida se efectuará, bien en un solo asiento si fuese de vencimiento único, bien en tantos asientos como vencimientos periódicos incumplidos existan señalando, en este caso, la fecha de cada uno de ellos.

4. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

5. El responsable del fichero deberá adoptar las medidas organizativas y técnicas necesarias que permitan acreditar la realización material del envío de notificación y la fecha de entrega o intento de entrega de la misma.

6. La notificación se dirigirá a la última dirección conocida del afectado a través de un medio fiable e independiente del responsable del fichero.

Norma tercera. *Cómputo del plazo de seis años que establece el artículo 28.3 de la Ley Orgánica.*

El cómputo del plazo a que se refiere el artículo 28.3 de la Ley Orgánica se iniciará a partir del momento de la inclusión del dato personal desfavorable en el fichero y, en todo caso, desde el cuarto mes, contado a partir del vencimiento de la obligación incumplida o del plazo en concreto de la misma si fuera de cumplimiento periódico.

CAPITULO II

Medidas de seguridad

Norma cuarta. *Forma de comprobación.*

1. Los sistemas que almacenen o procesen información relativa al cumplimiento o incumplimiento de obligaciones dinerarias deberán acreditar la efectiva implantación de las medidas de seguridad exigidas por el artículo 9.1 de la Ley Orgánica dentro del año siguiente a la publicación de la presente Instrucción. Para los ficheros que se inscriban con posterioridad a esta Instrucción, el plazo se computará a partir de la fecha en que aquélla se haya efectuado en el Registro General de Protección de Datos.

2. La implantación, idoneidad y eficacia de dichas medidas se acreditará mediante la realización de una auditoría, proporcionada a la naturaleza, volumen y características de los datos personales almacenados y tratados, y la remisión del informe final de la misma a la Agencia de Protección de Datos.

3. La auditoría podrá ser realizada:

a) Por el departamento de auditoría interna del responsable del fichero, si cuenta con un departamento formalmente constituido, profesionalmente cualificado e independiente del órgano responsable del tratamiento y gestión de los datos.

b) Por un auditor externo, profesionalmente cualificado e independiente del responsable del fichero.

4. La auditoría deberá ser realizada de acuerdo con las normas y recomendaciones de ejercicio profesional aplicables en el momento de su ejecución.

5. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles destinados a garantizar la integridad y confidencialidad de los datos personales almacenados o tratados, identificar sus deficiencias o insuficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basan los dictámenes alcanzados y recomendaciones propuestas.

6. Adicionalmente, los sistemas que almacenen o procesen información relativa al cumplimiento o incumplimiento de obligaciones dinerarias deberán someterse a una nueva auditoría tras la adopción de las medidas específicas que, en su caso, la Agencia determine, a resultas del informe inicial de auditoría. En todo caso, dichos sistemas deberán ser auditados periódicamente, a intervalos no mayores de dos años.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado».

§ 25

Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General

Agencia Española de Protección de Datos
«BOE» núm. 60, de 11 de marzo de 2019
Última modificación: 25 de junio de 2019
Referencia: BOE-A-2019-3423

Téngase en cuenta la sentencia del TC 76/2019, de 22 de mayo, por la que se declara contrario a la Constitución y nulo el apartado 1 del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado a ésta por la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Ref. BOE-A-2019-9548

La recopilación y tratamiento de datos por parte de las organizaciones políticas con fines de comunicación política junto con el uso de técnicas modernas como el big data y la inteligencia artificial han generado un amplio debate y preocupación respecto a los límites que deben aplicarse, entre los que se encuentra el derecho a la protección de datos de carácter personal.

De ahí que ya en la 27 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Montreux (Suiza), de 14 al 16 de septiembre de 2005, se aprobara la «Resolución sobre el Uso de Datos Personales para la Comunicación Política». En los últimos años dicha preocupación se ha incrementado, singularmente al hacerse públicos determinados casos de tratamiento ilícito de datos personales para influir en la opinión política de los votantes como el de Cambridge Analytica, lo que ha dado lugar a que diferentes autoridades nacionales de protección de datos hayan emitido sus criterios restrictivos al respecto. El 6 de marzo de 2014, la Autoridad Italiana de Protección de Datos (Garante para la Protezione dei Dati Personali) emitió su documento «Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall´informativa per fini di propaganda elettorale». En noviembre de 2016 lo hizo la Autoridad francesa (Commission Nationale de l'Informatique et des Libertés) con, entre otros, el título «Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?».

Y en abril de 2017 la Autoridad británica (Information Commissioner´s Office) aprobó su «Guidance on political campaigning».

Asimismo, el Supervisor Europeo de Protección de Datos emitió el 18 de marzo de 2018 su Opinión 3/2018 sobre «manipulación online y datos personales («EDPS Opinion on online manipulation and personal data») y la Comisión Europea, ante la proximidad de las elecciones al Parlamento Europeo, el pasado 12 de septiembre de 2018 aprobó su guía sobre la aplicación de la normativa europea de protección de datos en el contexto electoral («Commission guidance on the application of Union data protection law in the electoral context»).

Todos estos documentos muestran su preocupación sobre el uso del big data, la inteligencia artificial y la aplicación del microtargeting en los procesos electorales y que pueden llevar a la manipulación de las personas mediante la realización de perfilados exhaustivos y el fenómeno de las «fake-news» o «desinformación online». Por eso coinciden en la necesidad de garantizar la aplicación de la normativa de protección de datos en el contexto electoral.

Por su parte, el legislador español, a través de la disposición final tercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que entró en vigor el pasado 7 de diciembre, ha modificado la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG), introduciendo el artículo 58 bis con el fin de regular específicamente la recopilación y tratamiento de opiniones políticas por los partidos políticos así como el envío de propaganda electoral con el siguiente contenido:

> **«Artículo 58 bis.** *Utilización de medios tecnológicos y datos personales en las actividades electorales.*
>
> 1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.
>
> 2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.
>
> 3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.
>
> 4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.
>
> 5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»

El tratamiento de datos personales por parte de los partidos políticos, así como por el resto de sujetos que pueden presentar candidaturas en los procesos electorales, queda sujeto a la normativa general sobre protección de datos personales, actualmente constituida por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD) y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales incluida la modificación que ésta última ha hecho de la LOREG.

El informe del Gabinete Jurídico de esta Agencia de 19 de diciembre de 2018 ya destacaba que dicho precepto debía ser objeto de interpretación restrictiva al tratarse de una excepción al tratamiento de las categorías especiales de datos personales basado en el interés público que se ampararía en la letra g) del artículo 9.2 del RGPD. Además, el interés público actuaría como fundamento pero también como límite. Por tanto, la aplicación del mismo debe interpretarse siempre en el sentido más favorable a la consecución de dicho interés público, por lo que en ningún caso podrá amparar tratamientos, como el

microtargeting, que puedan ser contrarios a los principios de transparencia y libre participación que caracterizan a un sistema democrático.

Por otro lado, el legislador español ha hecho uso de la habilitación que concede el artículo 9.2.a) del RGPD disponiendo en el artículo 9.1. de la Ley Orgánica 3/2018 que «el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico». Por consiguiente, si el legislador español ha otorgado mayor protección a los datos relacionados con la ideología y al mismo tiempo ha establecido como única excepción al tratamiento de las opiniones políticas la contemplada en el citado artículo 58 bis de la LOREG, ha de ser objeto de interpretación restrictiva.

Asimismo, dicha interpretación restrictiva vendría avalada por la necesidad de que el artículo 58 bis sea interpretado conforme a lo establecido en la Constitución española y de modo que no conculque derechos fundamentales, como el derecho a la protección de datos de carácter personal reconocido en el artículo 18.4, el derecho a la libertad ideológica del artículo 16, la libertad de expresión e información del artículo 20 o el derecho a la participación política del artículo 23.

Por otro lado, el artículo 9.2.g) del RGPD requiere que se establezcan medidas adecuadas y específicas para proteger los intereses y derechos fundamentales de los afectados. Dichas garantías adquieren una especial relevancia tanto por la importancia de los datos personales objeto de tratamiento como por tratarse de tratamientos a gran escala de categorías especiales de datos que entrañarán un alto riesgo para los derechos y libertades de las personas físicas difícilmente mitigable si no se toman medidas adecuadas.

Precisamente por la existencia de un alto riesgo para los derechos y libertades de las personas físicas dichas garantías, al no haberse establecido por el legislador, deben identificarse por esta Agencia Española de Protección de Datos, en cumplimiento de las funciones de interpretación y aplicación de la normativa de protección de datos que le atribuyen los artículos 57 y 58 del RGPD, entre las que destacan las relativas a la evaluación de impacto, la consulta previa a la AEPD o la adopción de las oportunas medidas de seguridad. Todo ello sin perjuicio de cualquier otra que estime el responsable del tratamiento y las que puedan exigir otros órganos en el ámbito de sus competencias, como la Junta Electoral Central, el Tribunal de Cuentas, el Ministerio del Interior y, en último término, el Tribunal Constitucional.

Con la finalidad de fijar los criterios a los que responderá la actuación de esta autoridad en la aplicación de la normativa sobre protección de datos de carácter personal y de conformidad con lo dispuesto en los artículos 48.1 y 55 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, dispongo:

Artículo 1. *Ámbito objetivo.*

La presente Circular se aplica al tratamiento de datos personales relativos a opiniones políticas por los partidos políticos al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

Artículo 2. *Sujetos legitimados para realizar el tratamiento.*

1. Se encuentran legitimados para el tratamiento de los datos objeto de la presente circular, en el ámbito de la circunscripción que se corresponda con el proceso electoral al que se presenten, los partidos políticos, federaciones, coaliciones y agrupaciones de electores que presenten las correspondientes candidaturas y resulten proclamadas conforme a los artículos 43 y siguientes de la LOREG.

2. Dichos sujetos ostentarán la condición de responsables del tratamiento conforme al artículo 4.7) del RGPD.

3. El tratamiento de los datos podrá encomendarse a otro sujeto en calidad de encargado del tratamiento quien deberá ajustarse estrictamente a las instrucciones del responsable y previa suscripción del contrato previsto en el artículo 28 del RGPD.

4. Dichos datos no podrán ser comunicados ni transferidos a terceros.

Artículo 3. *Base jurídica del tratamiento.*

Solo será posible el tratamiento de datos personales que se refieran a opiniones políticas por los partidos políticos conforme al artículo 58 bis de la LOREG cuando concurra un interés público esencial conforme al artículo 9.2.b) del RGPD y se adopten las garantías adecuadas previstas en el artículo 7 de esta circular.

Los partidos políticos podrán tratar otro tipo de datos personales siempre que concurra alguna de las bases jurídicas del artículo 6 del RGPD y tratándose de categorías especiales, otra de las excepciones del artículo 9.2 RGPD, salvo el consentimiento del interesado conforme al artículo 9.1 de la Ley Orgánica 3/2018.

Artículo 4. *Marco en el que se habilita el tratamiento.*

1. El tratamiento de los datos al amparo del artículo 58 bis de la LOREG solo será lícito durante el periodo electoral y respecto de las actividades de propaganda y actos de campaña electoral reguladas en la sección 5.ª del capítulo VI del título I de la LOREG.

2. El responsable deberá determinar la finalidad o finalidades que se persiguen con el tratamiento, que en todo caso deberán guardar relación con su actividad electoral conforme a lo señalado en el apartado anterior.

Artículo 5. *Datos personales que pueden ser objeto de tratamiento.*

1. Solo podrán ser objeto de recopilación las opiniones políticas de las personas libremente expresadas por éstas en el ejercicio de sus derechos a la libertad ideológica y a la libertad de expresión reconocidos en los artículos 16 y 20 de la Constitución española.

2. En ningún caso podrán ser objeto de tratamiento otro tipo de datos personales a partir de los que, aplicando tecnologías como las de tratamiento masivo de datos o las de inteligencia artificial, se puede llegar a inferir la ideología política de una persona.

3. Las únicas fuentes de las que se pueden obtener los datos personales sobre opiniones políticas son las páginas web y aquellas otras fuentes que sean de acceso público.

Se entiende por fuentes de acceso público aquellas cuya consulta puede ser realizada por cualquier persona, quedando excluidas otro tipo de fuentes en las que el acceso está restringido a un círculo determinado de personas.

4. El tratamiento de cualquier otro tipo de datos personales u obtenidos de otras fuentes por los sujetos legitimados deberá ampararse en alguna de las bases legitimadoras del artículo 6 del RGPD y encontrarse en alguna de las excepciones del artículo 9.2 RGPD si se trata de categorías especiales de datos.

Artículo 6. *Actividades de tratamiento.*

1. Corresponderá al responsable determinar las actividades de tratamiento a realizar conforme al artículo 4.2) del RGPD que, en todo caso, deberán ser proporcionales al objetivo perseguido consistente en garantizar el adecuado funcionamiento de un sistema democrático, sin que sean admisibles tratamientos no proporcionales como el microtargeting ni los que tengan por finalidad forzar o desviar la voluntad de los electores. Tratándose de datos personales relativos a opiniones políticas, estos solo podrán ser objeto de recopilación conforme a lo previsto en el artículo 58 bis de la LOREG y el artículo 1 de esta Circular.

2. Si se pretende la elaboración de perfiles se deberá ser especialmente riguroso con el nivel de detalle y la exhaustividad del mismo, siendo admisible únicamente la elaboración de perfiles generales y por categorías genéricas, pero no la realización de perfiles individuales o realizados atendiendo a categorías muy específicas, de tal manera que sólo se puedan deducir patrones de conducta generales de la población de forma agregada, pero no de titulares de datos personales concretos.

3. En todo caso, resultarán de aplicación al tratamiento todos los principios recogidos en el artículo 5 del RGPD.

Artículo 7. *Garantías adecuadas.*

1. Conforme a lo previsto en el artículo 9.2.g) del RGPD tendrán la consideración de medidas adecuadas y específicas para proteger los intereses y derechos fundamentales de

los afectados, en todo caso, las siguientes, sin perjuicio de cualquier otra que estime el responsable del tratamiento y las que puedan exigir otros órganos en el ámbito de sus competencias:

1.º Atendiendo al principio de responsabilidad desde el diseño y por defecto previsto en el artículo 25 del RGPD, deberán adoptarse, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, e incluso la agregación y anonimización. Además, deberá garantizarse que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento y que no serán accesibles, sin intervención de la persona, a un número indeterminado de personas.

2.º Será obligatorio designar a un delegado de protección de datos conforme a lo previsto en el artículo 37.1.c) del RGPD, al realizarse un tratamiento a gran escala de categorías especiales de datos personales. El delegado de protección de datos desempeñará las funciones que le atribuyen el artículo 39 del RGPD y los artículos 36 y 37 de la LOPDPGDD con especial diligencia atendiendo al alto riesgo asociado a estos tratamientos.

3.º Deberá llevarse un registro de las actividades de tratamiento con el contenido señalado en el artículo 30 del RGPD, debiendo ser precisos y claros, conforme a los principios de lealtad y transparencia, en la descripción de los fines del tratamiento, y de las categorías de interesados y de datos personales objeto de tratamiento. La llevanza de dicho registro resultará en todo caso obligatoria al incluir categorías especiales de datos personales del artículo 9.

4.º Se deberá realizar una evaluación de impacto relativa a la protección de datos al realizarse un tratamiento a gran escala de las categorías especiales de datos conforme a lo dispuesto en el artículo 35.3 del RGPD.

5.º Deberá consultarse a la AEPD antes de proceder al tratamiento conforme al artículo 36.1 del RGPD al tratarse de tratamientos que entrañan un alto riesgo, a no ser que el responsable justifique la adopción de medidas para mitigarlo. En este último caso deberá remitirse a la AEPD el análisis de riesgos y la evaluación de impacto junto a la justificación de las medidas adoptadas, al amparo de lo previsto en el artículo 58.1. a) y e) del RGPD. La solicitud de consulta a la AEPD o, en su defecto, la remisión de la documentación anteriormente indicada, deberá realizarse al menos 14 semanas antes del inicio del periodo electoral.

6.º Deberán adoptarse las medidas de seguridad necesarias conforme a lo previsto en el artículo 32 del RGPD, que deberán ser lo más rigurosas que permita el estado de la técnica teniendo en cuenta que se están tratando datos referentes a las opiniones políticas cuyo tratamiento es excepcional y que suponen un alto riesgo para los derechos y libertades de las personas físicas.

7.º Cuando el tratamiento se vaya a realizar por un encargado del tratamiento, deberá seleccionarse uno que ofrezca garantías suficientes y haberse suscrito un contrato con el contenido del artículo 28 del RGPD, en el que deberá quedar plenamente garantizado que el encargado actuará solo siguiendo instrucciones del responsable, debiendo dichas instrucciones contemplar todas las garantías adecuadas a las que se hace referencia en la presente circular.

8.º Deberá facilitarse, de un modo sencillo y gratuito, el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición, conforme a lo previsto en el artículo 12 del RGPD y, en cuanto al derecho de oposición, conforme a lo previsto en el apartado 5 del artículo 58 bis de la LOREG.

9.º En el caso de que se pretenda obtener los datos de terceros que no actúen como encargados del tratamiento, el responsable deberá comprobar que dichos datos fueron obtenidos de manera lícita y cumpliendo con todos los requisitos del RGPD, especialmente que el tercero tiene una legitimación específica para obtener y tratar dichos datos y que ha informado expresamente a los afectados de la finalidad de cesión a los partidos políticos, cumpliendo de este modo con el principio general de responsabilidad proactiva consagrado en el artículo 5.2 del RGPD, y singularmente para actuar conforme a lo previsto en sus artículos 24 y 25.

10.º El responsable deberá cumplir con lo dispuesto en el artículo 22 del RGPD si los afectados van a ser objeto de decisiones automatizadas, incluida la elaboración de perfiles, siempre que el tipo de tratamiento que prevea, por sus características y teniendo en cuenta de nuevo la naturaleza de los datos tratados, pueda afectar significativamente a los ciudadanos.

2. El responsable del tratamiento y, en su caso, el encargado, deberán ser capaces de acreditar documentalmente la adopción de las anteriores garantías.

Artículo 8. *Deber de información.*

1. En todo caso deberá cumplirse con el deber de información previsto en los artículos 13 y 14 del RGPD, que deberá realizarse en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo de acuerdo con el artículo 12 del RGPD, siendo de aplicación lo previsto en el artículo 11 de la Ley Orgánica 3/2018.

2. Cuando se considere que la comunicación individual de dicha información a los afectados resulta imposible o suponga un esfuerzo desproporcionado, deberá facilitarse en forma electrónica en el sitio web del responsable, así como en las cuentas que tenga en redes sociales y servicios equivalentes.

3. Del mismo modo, cuando el responsable pretenda obtener los datos de un tercero, deberá comprobar que dicho tercero ha cumplido con su obligación de informar sobre los mismos extremos a los afectados, al menos de forma electrónica según lo indicado en al apartado anterior.

Artículo 9. *Momento en el que deberán adoptarse las garantías adecuadas.*

1. Antes del comienzo del periodo electoral los responsables que vayan a presentar las correspondientes candidaturas podrán realizar las actuaciones necesarias para preparar los tratamientos que vayan a desarrollar en el periodo electoral, conforme a las obligaciones señaladas en los artículos anteriores, pero sin poder iniciar los tratamientos. En especial, las relativas al registro de actividades, evaluación de impacto, consulta previa, designación del delegado de protección de datos si no lo hubieran designado con anterioridad y la celebración, en su caso, del contrato de encargado del tratamiento.

2. Durante el periodo electoral podrá iniciarse el tratamiento, debiendo en primer lugar cumplir con la obligación de información conforme al artículo 8 y velar por el cumplimiento de la normativa de protección de datos. En el caso de que los sujetos que hayan presentado candidaturas no resulten proclamados, deberá interrumpirse inmediatamente el tratamiento y procederse a la supresión de los datos conforme al apartado siguiente.

3. Terminado el periodo electoral deberá garantizarse la supresión de los datos personales conforme a lo establecido en la ISO 27001:2013 «Seguridad de la información» y la Norma UNE- EN15713:2010 «Destrucción del Material Confidencial. Código de Buenas Prácticas», o cualquier otra metodología de reconocido prestigio para la destrucción de la información debidamente documentada, procediéndose al bloqueo de los mismos cuando proceda de conformidad con el artículo 32 de la Ley Orgánica 3/2018.

Artículo 10. *Violación de la seguridad de los datos personales que se refieran a opiniones políticas.*

1. En caso de violación de la seguridad de los datos personales que se refieran a opiniones políticas, el responsable del tratamiento deberá notificarlo, en todo caso, a la Agencia Española de Protección de datos conforme al artículo 33 del RGPD al constituir un riesgo para los derechos y libertades de las personas físicas.

2. Asimismo, deberá comunicarlo a los afectados salvo que se cumpla alguna de las condiciones del artículo 34.3 del RGPD.

Artículo 11. *Envío de propaganda electoral por medios electrónicos o sistemas de mensajería y contratación de propaganda electoral en redes sociales o medios equivalentes.*

1. Conforme al apartado 3 del artículo 58 bis el envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en

redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

2. Los datos personales que vayan a ser utilizados por los partidos políticos, federaciones, coaliciones o agrupaciones de electores para el envío de propaganda electoral tales como números de teléfono, correo electrónico u otros similares deberán haber sido obtenidos lícitamente, amparados en alguna de las bases jurídicas del artículo 6 del RGPD y deberán corresponder a personas que puedan ejercer su derecho al voto en el ámbito de la circunscripción que se corresponda con el proceso electoral al que se presenten

3. En todo caso, en los envíos que se realicen deberá constar su carácter electoral y la identidad del remitente. Asimismo, deberá facilitarse de un modo sencillo y gratuito el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición, con especial atención en el caso de este último, conforme al apartado 5 del artículo 58 bis de la LOREG.

En caso de ejercicio del derecho de oposición, los datos personales dejarán de ser tratados para el envío de propaganda electoral mientras el afectado no preste su consentimiento expreso.

Disposición transitoria única. *Consulta previa a la AEPD o remisión de la documentación prevista en el artículo 7.1. 5.º en los procesos electorales previstos para el 28 de abril y el 26 de mayo de 2019.*

En los procesos electorales previstos para el 28 de abril y el 26 de mayo de 2019 la consulta previa o la remisión de la documentación a la que se refiere el artículo 7. 1. 5.º de la presente Circular deberá realizarse, en su caso, con una antelación mínima de tres semanas al inicio de la campaña electoral, debiendo emitirse el correspondiente informe o adoptarse las medidas oportunas con anterioridad al inicio de la misma.

Disposición final. *Entrada en vigor.*

La presente Circular entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 26

Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, de conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de esos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio

Agencia Española de Protección de Datos
«BOE» núm. 265, de 5 de noviembre de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-18134

PREÁMBULO

I

Desde la aprobación en 2016 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, o RGPD), y con la finalidad de asistir y formar a todos los actores implicados en los procesos de tratamiento de datos y procurar una transición ordenada a la nueva regulación establecida en el RGPD, la Agencia Española de Protección de Datos (AEPD) ha venido desarrollando funciones consultivas particularizadas, a demanda de responsables y encargados individuales. Transcurridos más de cinco años desde la entrada en vigor del RGPD parece oportuno concluir la fase transitoria y definir con claridad, en aras de la certeza jurídica de los sujetos obligados, cuáles son las funciones consultivas que debe desarrollar la AEPD, de conformidad con el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD), y su Estatuto, aprobado por el Real Decreto 389/2021, de 1 de junio.

El objeto de la presente Instrucción es adaptar las funciones consultivas de la AEPD a los preceptos del RGPD, la LOPDPGDD y de su Estatuto. De una parte, se trata de ajustar la actividad de la AEPD al principio de responsabilidad proactiva de los responsables del tratamiento enunciado como novedad en el RGPD y, de otra, respetar el principio de

competencia administrativa y ceñirse a las funciones previstas en el citado RGPD (artículo 57) para las autoridades de control en protección de datos.

En cuanto al principio de responsabilidad proactiva de los responsables del tratamiento, efectivamente, tal como se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, «la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan»; con el asesoramiento y supervisión, en su caso, del Delegado de Protección de Datos (DPD). Este nuevo principio, esencial para entender el marco normativo de la protección de datos personales en la Unión Europea (UE), está recogido en el artículo 5 del RGPD, en concreto en el apartado 2.f), que establece que: «el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 [los principios de obligada observancia recogidos en el RGPD] y capaz de demostrarlo (responsabilidad proactiva)».

De lo anterior se deduce que tanto el RGPD, como la LOPDGDD en el ámbito nacional, han establecido un nuevo sistema de cumplimiento para responsables y encargados de tratamiento por el cual estos sujetos no sólo deben cumplir las obligaciones que les impone la normativa aplicable, sino que proactivamente deben poder demostrarlo o documentarlo frente a las autoridades de control. El RGPD ofrece un conjunto de medidas que facilitan su cumplimiento, unas de carácter obligatorio –en determinados supuestos– como la designación de un delegado de protección de datos (DPD), que proporciona asesoramiento a responsables y encargados del tratamiento y supervisa el cumplimiento del RGPD, y otras voluntarias como los códigos de conducta o los mecanismos de certificación.

Asimismo, hay que tener en cuenta la nueva competencia atribuida a la Presidencia de la AEPD por el artículo 55 de la LOPDGDD, que la faculta para dictar circulares que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el RGPD y en la LOPDGDD, y que serán obligatorias una vez publicadas en el «Boletín Oficial del Estado», ajustándose su procedimiento de elaboración a lo establecido en el Estatuto de la Agencia Española de Protección de Datos. Atendiendo a dicha competencia y al carácter obligatorio de las circulares, se considera que las mismas deben configurarse como el elemento prioritario a través del cual la AEPD establezca los criterios generales de interpretación de la normativa sobre protección de datos personales, contribuyendo de este modo a incrementar la seguridad jurídica.

II

El segundo elemento de adaptación, ajustar la actividad de la AEPD al catálogo de funciones previstas en el RGPD para las autoridades de control, es un elemento ligado también al nuevo principio de responsabilidad proactiva. En este enfoque, las autoridades de control tienen un carácter marcadamente de supervisión y no se encuentran entre sus funciones, listadas en el artículo 57 del RGPD, las de asesorar o resolver las consultas de los responsables o encargados del tratamiento, porque son ellos mismos, asistidos por sus DPD, o abogados o consultores, quienes han de determinar los tratamientos de datos que implique el ejercicio de su actividad, evaluar los riesgos que su suponen para los derechos y libertades de los afectados e implantar las medidas necesarias para evitarlos o reducirlos. Así lo ha interpretado acertadamente la Comisión Europea en sus orientaciones sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018, contenidas en su Comunicación 43 de fecha 24 de enero de 2018. A juicio de la Comisión Europea, el asesoramiento jurídico personalizado e individualizado a los responsables y los encargados del tratamiento sólo corresponde a los abogados y delegados de protección de datos. Conviene subrayar también que la LOPDGDD tampoco ha ampliado las funciones listadas en el citado artículo 57 del RGPD, ni ha dado cobertura legal por tanto a una función consultiva dirigida a responsables o encargados del tratamiento.

Además, se ha de tener en cuenta el carácter independiente e imparcial que las autoridades de control en protección de datos deben observar en el ejercicio de su función primordial supervisora, por lo que el asesoramiento particularizado a responsables o encargados podría perjudicar en un futuro la imparcialidad de las labores de supervisión,

cuando se hubiese asesorado previamente sobre un tratamiento de datos que posteriormente da lugar a actuaciones de investigación.

III

En consecuencia, las funciones consultivas de la AEPD deben adaptarse al nuevo esquema jurídico creado por el RGPD, que no contempla el asesoramiento individualizado a responsables o encargados por la autoridad de control ni la consulta particular a demanda de los responsables. Por tanto, la AEPD no desarrollará funciones consultivas individualizadas destinadas a responsables y encargados del tratamiento, porque no se prevé así en el RGPD ni en la LOPDGDD. No es coherente con el principio de responsabilidad proactiva y puede generar una percepción de falta de imparcialidad cuando la AEPD tenga que ejercitar sus potestades de investigación y supervisión sobre tratamientos en los que previamente ha desarrollado una función asesora o consultiva.

Por otro lado, es criterio reiterado de esta Agencia el de no atender a las consultas que puedan plantearse por despachos de abogados o consultores cuyas funciones son, precisamente, la interpretación de la ley y el asesoramiento a sus clientes.

No obstante, para ayudar de manera generalizada al cumplimiento de responsables y encargados, la AEPD ha publicado, desde la aprobación del RGPD, numerosas guías, manuales de ayuda y diseñado aplicaciones gratuitas y disponibles en su web (www.aepd.es), que facilitan a los responsables y encargados la puesta en marcha de su actividad con respeto de la normativa de protección de datos y la evaluación de los riesgos generados. Asimismo, la AEPD pone a disposición de todos en su web un catálogo de preguntas frecuentes donde puede encontrarse respuesta a los problemas más comunes detectados en la aplicación y cumplimento de la normativa de protección de datos.

Con base en todo lo anterior, las funciones consultivas de la AEPD, según estipula el RGPD y la LOPDGDD, se configuran esencialmente para los siguientes supuestos: en primer lugar, se establecen funciones consultivas relacionadas con la actividad normativa, tanto legislativa como reglamentaria. En segundo lugar, se establecen también funciones informativas dirigidas a las personas interesadas o ciudadanos, cuando éstos las soliciten, para informarse sobre sus derechos en materia de protección de datos. En tercer lugar, la AEPD puede ser consultada por los DPD bajo ciertos requisitos coherentes con el principio de responsabilidad proactiva. Finalmente, se regula la función consultiva específica, contemplada en el artículo 36 del RGPD, cuando las conclusiones de una evaluación de impacto muestren que el tratamiento al que se refiere entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

Por tanto, son las funciones consultivas descritas en el párrafo anterior las que está obligada a realizar la AEPD, dentro del marco competencial fijado por el RGPD y la LOPDGDD, y las que se regulan en las normas de la presente instrucción.

IV

El considerando 38 del RGPD señala que «Los niños merecen una protección específica de sus datos personales» y el artículo 57.1.b) establece que «Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención». Para este grupo la AEPD dispone de un espacio en su web dedicado exclusivamente al tratamiento de los datos personales de los menores y al ámbito educativo, que incluye un canal específico de atención y consulta que, en aras de la particular protección de la que son acreedores los menores, ha de continuar prestando sus servicios en las condiciones en las que se viene realizando, por lo que la presente instrucción no debe afectar a su actual funcionamiento y operatividad.

En consecuencia con lo expuesto, en virtud de la facultad que me concede el artículo 13.1, letras a) y d), del Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, y el artículo 6 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, apruebo la siguiente

Instrucción

Primero. *Objeto y ámbito de aplicación.*

1. La presente instrucción será de aplicación a la actividad consultiva de la AEPD que comprende las siguientes funciones:

a) Informar preceptivamente:

1. Los proyectos de disposiciones generales de desarrollo del RGPD y de la LOPDGDD.
2. Cualesquiera anteproyectos de ley o proyectos de reglamento que incidan en la materia propia del RGPD.
3. Los anteproyectos de ley por los que se exijan datos con carácter obligatorio y su adecuación a lo dispuesto en el artículo 7 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.
4. El contenido y formato de los cuestionarios, hojas censales y otros documentos de recogida de datos con fines estadísticos oficiales.
5. Los procesos de recogida y tratamiento de los datos personales a efectos estadísticos oficiales.
6. Las condiciones de seguridad de los tratamientos realizados con fines exclusivamente estadísticos oficiales.
7. Cualesquiera otros informes que se deban emitir por la AEPD con carácter preceptivo en virtud de disposiciones legales o reglamentarias.

b) Proporcionar información relativa a las consultas formuladas por las personas afectadas sobre el ejercicio de sus derechos, cuando éstas así lo soliciten en virtud del artículo 57.1.e) del RGPD.

c) Dar respuesta a las consultas presentadas por los DPD, cuando estos lo soliciten en virtud del artículo 39.1.e) del RGPD y conforme a los requisitos que se exponen en la norma 4.

d) Dar respuesta a consultas previas presentadas por los responsables del tratamiento conforme dispone el artículo 36 del RGPD [artículo 57.1.l) RGPD].

2. Asimismo, la presente instrucción comprende las actuaciones para promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del RGPD. Tales actuaciones consistirán en:

1. La elaboración de materiales, recursos y herramientas dirigidos a facilitar y ayudar a los responsables y encargados el cumplimiento del RGPD y la LOPDPGDD.
2. La elaboración y ejecución de planes de acción dirigidos a sectores cuya actividad principal implique el tratamiento de datos personales, a organizaciones de consumidores y usuarios, y representativas de trabajadores.
3. No es objeto de la presente instrucción las circulares que puede dictar la Agencia para establecer los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el RGPD y en la LOPDGDD, que se ajustarán al procedimiento regulado en el Estatuto.

CAPÍTULO I

Función consultiva dirigida al Parlamento, al Gobierno y a las Administraciones Públicas relativa al desarrollo y aplicación de las normas que incidan en materia propia del RGPD y la LOPDPGDD [artículo 57.1.e) RGPD]

Segundo. *El Gabinete Jurídico de la Agencia Española de Protección de Datos.*

1. Al Gabinete Jurídico de la Agencia Española de Protección de Datos le corresponde el asesoramiento jurídico de los distintos órganos de la Agencia, en virtud del Convenio suscrito con la Abogacía General del Estado-Dirección del Servicio Jurídico del Estado, que ejercerá en los términos establecidos por la Ley 52/1997, de 27 de noviembre, de Asistencia Jurídica al Estado e Instituciones Públicas, su normativa de desarrollo y el citado Convenio.

Este asesoramiento, que incluirá el correspondiente a los informes preceptivos sobre disposiciones legales y reglamentarias que le sean solicitados por la Presidencia de la Agencia, tendrá carácter prioritario y será preferente sobre cualesquiera otros asuntos que le puedan ser sometidos a su consideración.

Asimismo, le corresponderá emitir informe en aquellos otros asuntos de carácter jurídico en los que deba consultarse, preceptivamente, a la Agencia Española de Protección de Datos, en virtud de disposiciones legales o reglamentarias, y no sean competencia de otro órgano de la Agencia, que tendrán preferencia sobre el resto de consultas que puedan formularse sin dicho carácter.

2. Corresponderá al Gabinete Jurídico informar las consultas que puedan presentar los DPD conforme a la norma 4, cuando se trate de cuestiones que no puedan resolverse con los criterios ya informados por la AEPD o de cuestiones nuevas derivadas de la aplicación del nuevo régimen jurídico de protección de datos de carácter personal, siempre que el Gabinete Jurídico considere que tienen un alcance general en el que resulte conveniente un informe que contribuya a la seguridad jurídica.

En estos supuestos, el informe del DPD deberá analizar detallada y motivadamente las cuestiones objeto de consulta, incluyendo el criterio defendido por el propio DPD, así como el razonamiento sobre el alcance general de la consulta.

3. Estas consultas se atenderán atendiendo a la relevancia de las mismas, en la medida en que el resto de la actividad del Gabinete a la que se refieren los apartados anteriores lo permitan, dando preferencia a las que formulen los DPD de las Administraciones Públicas y de las asociaciones y organizaciones representativas de categorías de responsables o encargados.

4. En ningún caso se emitirán informes sobre consultas que se refieran a tratamientos que estén realizando sujetos distintos del propio consultante, sin perjuicio de su derecho a presentar una reclamación conforme al artículo 77.1 del RGPD.

5. Con carácter excepcional y siempre que el Gabinete Jurídico considere que tienen un alcance general en el que resulte conveniente un informe que contribuya a la seguridad jurídica, se atenderán las consultas que formulen los responsables o encargados del tratamiento, en los supuestos en que no sea obligatoria designación de DPD, siempre que se justifique la imposibilidad de su designación con carácter voluntario y se acompañe un informe que analice detallada y motivadamente las cuestiones objeto de consulta. En estos supuestos, se dará preferencia a las formuladas por organizaciones representativas de categorías de responsables o encargados.

CAPÍTULO II

Función consultiva dirigida a los ciudadanos para facilitar información sobre el ejercicio de sus derechos [artículo 57.1.e) RGPD]

Tercero. *Cauces de información de la AEPD a los ciudadanos sobre sus derechos, contenidos y efectos de la actividad informativa.*

1. El órgano de la AEPD responsable de la promoción informativa es la Subdirección General de Promoción y Autorizaciones (SGPA).

2. La SGPA proporciona el servicio de información a los ciudadanos sobre sus derechos a través de los siguientes mecanismos:

a) Publicaciones informativas a través de la web de la AEPD (FAQ, guías, manuales y otros materiales y contenidos).

b) Atención presencial concertada mediante cita previa.

c) Atención telefónica individualizada.

d) Resolución de consultas escritas de ciudadanos interesados a través de la aplicación disponible en la sede electrónica de la AEPD para consultas individualizadas.

3. Las condiciones y horarios de la atención presencial y telefónica se fijan en la web de la AEPD.

4. La atención telefónica y la presencial garantizará la información sobre sus derechos de protección de datos a aquellos ciudadanos que no tienen acceso o no disponen de medios electrónicos.

5. Las consultas que se formulen ante la AEPD deben referirse a los derechos de la persona solicitante. Las respuestas a las consultas constituyen una actividad meramente informativa del órgano administrativo, no incluyen valoraciones sobre tratamientos realizados por terceros, ni modifican en modo alguno la situación jurídica del solicitante.

6. Por razones de eficiencia administrativa, si una consulta individual formulada por escrito se encuentra respondida ya en el catálogo de preguntas frecuentes, la SGPA no repetirá nuevamente la información y se indicará al solicitante la FAQ que responde a esa pregunta.

7. El catálogo de preguntas frecuentes estará disponible en la web de la AEPD, se mantendrá actualizado y adaptado a la evolución tecnológica y a las disposiciones y necesidades económicas y sociales del momento.

8. Sin perjuicio de lo previsto en las normas 6 y 7, el servicio de consultas de atención al ciudadano no atenderá las formuladas individualmente por responsables o encargados del tratamiento ni por abogados ni consultores.

CAPÍTULO III

Función consultiva dirigida a los Delegados de Protección de Datos (DPD) conforme al artículo 39.1.e) del RGPD

Cuarto. *Consultas de los DPD.*

1. La AEPD ha habilitado un canal de consulta para DPD, dependiente orgánicamente de la SGPA.

2. Las consultas por escrito que formulen los DPD, al amparo de lo previsto en el artículo 39.1.e) del RGPD deberán remitirse al canal DPD a través de su sede electrónica.

3. Para la formulación de las consultas el DPD deberá haber sido previamente comunicado a la AEPD por el responsable o encargado. La inclusión en la relación de DPD de la AEPD será suficiente para acreditar su designación como DPD.

4. Las consultas deben ir acompañadas de un informe del DPD en cuestión, en el que se analice el tratamiento sobre el que se consulta y se examinen los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del mismo. Todo ello de conformidad con el principio de responsabilidad proactiva y el artículo 39.2 del RGPD. Las consultas que no vengan acompañadas por el informe del DPD que la remite no serán atendidas.

5. No serán objeto de respuesta las consultas:

a) Que planteen tratamientos hipotéticos.

b) Que estén o puedan estar relacionadas con procedimientos en tramitación en la AEPD, incluidas las relativas al estado de tramitación.

c) Que pretendan la validación de actuaciones o documentos en materia de protección de datos elaborados por responsable o encargados.

d) Que impliquen acceso a la información pública.

e) Que se refieran a cuestiones que se encuentran ya explicadas y son accesibles en los materiales publicados en la página web de la AEPD, tales como las Guías, Preguntas Frecuentes y Herramientas elaboradas para facilitar el cumplimiento del RGPD.

6. Este Canal también estará disponible para las organizaciones y asociaciones representativas de responsables y encargados del tratamiento que presten servicio de asesoramiento en materia de protección de datos a sus asociados, especialmente cuando se trate de pequeñas y micro empresas, en las mismas condiciones que se establecen para los DPD.

7. Las consultas serán contestadas por escrito. Alternativamente, por razones de eficiencia administrativa, si se observa la presentación de múltiples consultas formuladas por diferentes DPD sobre el mismo objeto, o de un determinado sector de actividad, la SGPA puede organizar una actividad interactiva con los DPD o las organizaciones y asociaciones

afectadas a fin de examinar y resolver todas las consultas simultáneamente en una sola actividad.

CAPÍTULO IV

Función consultiva sobre las operaciones de tratamiento contempladas en el artículo 36.2 del RGPD [artículo 57.1.l) RGPD]

Quinto. *Consultas sobre las operaciones de tratamiento de alto riesgo.*

1. Serán objeto de consulta previa las evaluaciones de impacto relativas a la protección de datos (EIPD) de aquellos tratamientos que, cumpliendo con los principios y derechos establecidos en el RGPD, sean de alto riesgo para los derechos y libertades de los interesados, y cuando el responsable no haya podido mitigar o evitar dicho riesgo. Además, también aquellos tratamientos sometidos a la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales que, cumpliendo con los principios y derechos establecidos en la norma, la EIPD indique que el tratamiento entrañaría un alto nivel de riesgo, a falta de medidas adoptadas por el responsable para mitigar el riesgo o los posibles daños, o cuando el tipo de tratamiento pueda generar un alto nivel de riesgo para los derechos y libertades de los interesados, en particular, cuando se usen tecnologías, mecanismos o procedimientos nuevos.

2. La consulta previa solo se podrá realizar antes de proceder al tratamiento de datos personales, excepto cuando se produzcan en el tratamiento cambios en su naturaleza, alcance, contexto o riesgos que sean ajenos al responsable.

3. En el caso de que haya obligación de designar un DPD, la consulta previa solo se podrá presentar cuando éste haya sido designado y comunicado a la AEPD previamente a la remisión de la consulta.

4. El contenido mínimo para realizar una solicitud de consulta previa incluirá lo exigido en el artículo 36.3 del RGPD:

a) «Las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial»,

b) «los fines y medios del tratamiento previsto»,

c) «las medidas y garantías para proteger los derechos y libertades de los interesados»,

d) «en su caso, los datos de contacto del delegado de protección de datos»,

e) «la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y»

f) «cualquier otra información que solicite la autoridad de control».

5. Con relación a la documentación de la evaluación de impacto relativa a la protección de datos establecida en la letra «e» del artículo 36 apartado 3, el contenido mínimo incluirá, al menos:

a) Identificación del tratamiento y, en su caso, de la versión del mismo a la que corresponde la EIPD.

b) Fecha, firma y datos de contacto del responsable del tratamiento, de quien ha elaborado la documentación de la EIPD y, en caso de que exista o deba existir DPD, fecha, firma y datos de contacto del DPD.

c) En el caso de que se haya presentado previamente una consulta previa sobre el mismo tratamiento, sumario de las modificaciones introducidas en la naturaleza, contexto, ámbito, fines, riesgos y garantías del tratamiento.

d) Descripción del contexto interno y externo de la organización en la que se desenvuelve el tratamiento y la EIPD.

e) Identificación inequívoca y datos de contacto de todos los intervinientes en el tratamiento con sus roles.

f) Demostración del cumplimiento en el tratamiento de los principios y derechos establecidos en el RGPD, en particular, de una base jurídica.

g) Descripción sistemática del tratamiento.

h) Factores que determinan la realización de la EIPD y de la consulta previa.

i) Descripción del proceso de gestión formal de los riesgos para los derechos y libertades de los interesados, en particular, la identificación de los factores de riego, su análisis, la evaluación del nivel de riesgo del tratamiento y los mecanismos y garantías introducidos para minimizarlos incluyendo:

i. Las medidas establecidas sobre el concepto y diseño del tratamiento,
ii. las medidas de gobernanza y políticas de protección de datos,
iii. las medidas de protección de datos desde el diseño,
iv. las medidas de protección de datos por defecto,
v. la relación de activos y las medidas de seguridad para la protección de los derechos y libertades de los interesados.

j) En su caso, el análisis de la opinión de los interesados o de sus representantes en relación con el tratamiento previsto.

k) La evaluación objetiva y positiva de la necesidad y proporcionalidad del tratamiento.

l) Criterios para reevaluar la EIPD y, en su caso, de caducidad del tratamiento.

m) Cualquier otra documentación adicional necesaria para proporcionar a la autoridad de control la información completa y exacta sobre el tratamiento.

El desarrollo de la documentación de la EIPD deberá contemplar lo señalado por la AEPD en sus guías y recomendaciones, en particular, lo señalado en la guía «Gestión del riesgo y evaluación de impacto en tratamientos de datos personales» disponible en la web de la AEPD.

6. Las consultas previas deberán estar firmadas por el responsable y tendrán entrada en esta Agencia a través del canal de consultas previas dispuesto por la AEPD en su sede electrónica.

7. No tendrán consideración de consulta previa la documentación remitida sobre tratamientos que en los que no se cumplen los apartados del 1 al 6 de este artículo.

CAPÍTULO V

Actividades de información y sensibilización

Sexto. *Actividades de información activa.*

La AEPD elabora y ofrece en su web contenidos, materiales, documentos, preguntas y respuestas frecuentes (FAQ), guías, manuales, recursos y herramientas destinados a informar sobre el RGPD, la LOPDPGDD y demás normativa en materia de protección de datos, y a facilitar y ayudar a su cumplimiento.

Dichos materiales serán objeto de revisión y actualización periódica y, en todo caso, cuando se requiera por una modificación legislativa o decisión judicial.

Séptimo. *Actividades de sensibilización dirigidas a responsables y encargados sobre cumplimiento de obligaciones de protección de datos.*

La AEPD adoptará planes de acción bienales dirigidos a promover la sensibilización de los responsables y encargados del tratamiento sobre las obligaciones que establece el RGPD y a facilitar su cumplimiento.

Los planes de acción incluirán, entre otras medidas, la organización y celebración de jornadas, sesiones, seminarios, reuniones, tanto presenciales como online, y webinarios por sectores concretos de actividad.

Para su efectividad tendrá en cuenta los asuntos que le trasladen las asociaciones y organizaciones representativas de los responsables y encargados del tratamiento de cada sector, así como aquellas otras que se hayan puesto de manifiesto de manera reiterada a través del Canal del DPD, o como consecuencia del ejercicio de las potestades de la AEPD.

En la elaboración de los planes de acción la AEPD podrá establecer alianzas con dichas asociaciones y organizaciones, así como con aquellas instituciones y entidades representativas de los sectores de interés.

En los planes de acción se prestará una especial atención a las organizaciones que representen a las pequeñas empresas y microempresas.

Disposición adicional única. *Memoria anual.*

La AEPD incluirá en su Memoria anual información estadística sobre la actividad consultiva de la AEPD e informará sobre los cambios en los canales electrónicos de comunicación, si los hubiese.

Disposición final. *Entrada en vigor.*

Esta instrucción entrará en vigor el día siguiente al de su publicación.

§ 27

Circular 1/2023, de 26 de junio, sobre la aplicación del artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones

Agencia Española de Protección de Datos
«BOE» núm. 153, de 28 de junio de 2023
Última modificación: sin modificaciones
Referencia: BOE-A-2023-15071

La Ley 11/2022, de 28 de junio, General de Telecomunicaciones, publicada en el «Boletín Oficial del Estado» de 29 de junio de 2022, dedica el apartado 1 de su artículo 66 a regular el derecho de los usuarios finales a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas, incluyendo en su letra b) el derecho a no recibir llamadas no deseadas, con las excepciones que el mismo precepto contempla:

1. Respecto a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas los usuarios finales de los servicios de comunicaciones interpersonales disponibles al público basados en la numeración tendrán los siguientes derechos:

[…]

b) a no recibir llamadas no deseadas con fines de comunicación comercial, salvo que exista consentimiento previo del propio usuario para recibir este tipo de comunicaciones comerciales o salvo que la comunicación pueda ampararse en otra base de legitimación de las previstas en el artículo 6.1 del Reglamento (UE) 2016/679 de tratamiento de datos personales.

Dicha regulación se completa con la previsión respecto de su entrada en vigor, que se contiene en el apartado segundo de la disposición final sexta:

2. El derecho de los usuarios finales a no recibir llamadas no deseadas con fines de comunicación comercial contemplado en el artículo 66.1.b) entrará en vigor en el plazo de un año a contar desde la publicación de la presente ley en el «Boletín Oficial del Estado». Hasta ese momento, los usuarios finales de los servicios de comunicaciones interpersonales disponibles al público basados en la numeración podrán seguir ejercitando el derecho a oponerse a recibir llamadas no deseadas con fines de comunicación comercial que se efectúen mediante sistemas distintos de los establecidos en el artículo 66.1.a) y a ser informados de este derecho.

Esta nueva regulación implica un cambio sustancial respecto del régimen jurídico aplicable bajo la vigencia de la derogada Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, cuyo artículo 48.1.b. reconocía a los usuarios finales el derecho «a oponerse a recibir llamadas no deseadas con fines de comunicación comercial que se efectúen mediante sistemas distintos de los establecidos en la letra anterior y a ser informado de este derecho», haciendo primar el derecho de los usuarios finales a no recibir

dichas llamadas y la consiguiente obligación de los responsables de no realizarlas, salvo que acrediten la concurrencia de alguna de las excepciones contempladas en la norma que, dado su carácter excepcional, deben ser objeto de interpretación restrictiva.

Como consecuencia de las dudas suscitadas respecto de la interpretación del nuevo artículo 66.1.b) de la vigente Ley General de Telecomunicaciones, a petición de la Directora de la Agencia Española de Protección de Datos, el Gabinete Jurídico emitió el informe 40/2022 en el que, atendiendo a que el citado artículo no ha limitado exclusivamente la realización de las llamadas con fines de comunicación comercial al previo consentimiento de los usuarios finales, sino que ha incluido la posibilidad de que puedan ampararse en otras bases jurídicas del artículo 6.1. del RGPD, concluía que el precepto admite, como base legitimadora, además del consentimiento, el interés legítimo, recomendando que, ante las dudas suscitadas y con la finalidad de contribuir a la seguridad jurídica, se aprobara una circular.

Con la finalidad de fijar los criterios a los que responderá la actuación de esta autoridad en la aplicación de la normativa sobre protección de datos de carácter personal, la presente circular delimita su ámbito de aplicación, referido al derecho de los usuarios finales de los servicios de comunicaciones interpersonales disponibles al público basados en la numeración a no recibir llamadas no deseadas con fines de comunicación comercial contemplado en el artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, el cual resulta de aplicación a todos los responsables del tratamiento que realicen llamadas comerciales, con independencia del sector al que pertenezcan, al tratarse de una normativa referida a los derechos de los consumidores y usuarios que se aplica de manera general a cualquier empresa o empresario que utilice aquellos servicios y no solamente a las compañías operadoras en el sector.

Asimismo, se procede a concretar las bases jurídicas aplicables al tratamiento de los datos personales conforme al artículo 6.1. del Reglamento (UE) 2016/679, que según el criterio de esta Agencia quedarían limitadas, además de al consentimiento del afectado, al interés legítimo previsto en su letra f), al no resultar de aplicación, conforme a reiterada doctrina de esta Agencia, la base contractual de la letra b) por tratarse de tratamientos que no son necesarios para la ejecución del contrato, ni concurrir los demás supuestos contemplados en dicho precepto.

En relación con la base jurídica del interés legítimo, se considera necesario establecer criterios que faciliten la realización de la ponderación por el responsable teniendo en cuenta la finalidad restrictiva de la nueva regulación, estableciéndose una presunción *iuris tantum* de prevalencia del interés legítimo del responsable que operará en los supuestos en los que se cumplan los requisitos contenidos en la misma, y que se corresponden con los contemplados en el artículo 21.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, al existir identidad de razón. La ausencia de alguno de los requisitos señalados impedirá que opere la citada presunción. Asimismo, se especifica que dicha presunción no ampara la comunicación de los datos personales a otras empresas del grupo con fines comerciales, al requerir este tratamiento el consentimiento específico previo del usuario.

Por otro lado, se especifica que la nueva regulación introducida por el artículo 66.1.b) de la Ley 11/2022, de 28 de junio ha venido a poner fin a la práctica generalizada de realizar llamadas comerciales a números generados de forma aleatoria sin el consentimiento previo del usuario, al no poder valorarse en estos supuestos, dada la ausencia de otros datos personales, la posible prevalencia de los intereses, derechos y libertades de los afectados.

Asimismo, se especifica que los números de teléfono obrantes en las guías de abonados únicamente podrán utilizarse respecto de aquellos abonados que hayan prestado su consentimiento expreso para su uso con fines comerciales lo que deberá figurar, con carácter general, en las correspondientes guías. Tratándose de números correspondientes a personas físicas que presten servicios en personas jurídicas o de empresarios individuales y de profesionales liberales que puedan figurar en dichas guías o en otros instrumentos similares, operará la presunción contenida en el artículo 19 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales en cuanto se refiera a la oferta de productos y servicios relacionados con la actividad profesional o empresarial y no se trate de entablar relación en cuanto tales personas físicas.

Por último, se identifican otras garantías específicas que, según el criterio de esta Agencia, contribuyen a reforzar la licitud del tratamiento, referidas al deber de informar y a la forma de retirar el consentimiento o ejercer el derecho de oposición, incluida la grabación de las llamadas conforme al principio de responsabilidad proactiva como forma de acreditar el cumplimiento de los requisitos establecidos en la presente circular.

Por ello y de conformidad con lo dispuesto en los artículos 48.1 y 55 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y en el artículo 6 del Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, de acuerdo con el Consejo de Estado, dispongo:

Artículo 1. *Objeto.*

1. La presente circular tiene por objeto fijar los criterios a que responderá la actuación de la AEPD en relación con el derecho de los usuarios finales de los servicios de comunicaciones interpersonales disponibles al público basados en la numeración a no recibir llamadas no deseadas con fines de comunicación comercial, independientemente del sector al que pertenezca el responsable, salvo que exista consentimiento previo del propio usuario para recibir este tipo de comunicaciones comerciales o salvo que la comunicación pueda ampararse en otra base de legitimación de las previstas en el artículo 6.1 del Reglamento (UE) 2016/679, de conformidad con lo previsto en el artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

2. No son objeto de la presente circular cualesquiera otros tratamientos de datos personales, distintos a los necesarios para la realización de la llamada con fines de comunicación comercial, que puedan realizarse por el responsable vinculados a la misma finalidad comercial, como puedan ser los relacionados con la obtención de datos de contacto procedentes de terceros, el posible perfilado de los contactos y su segmentación, el enriquecimiento de datos con, entre otros, las respuestas que esté dando el cliente o su posible grabación con estos fines, los cuales requerirán contar con la correspondiente base legitimadora conforme al artículo 6.1. del Reglamento (UE) 2016/679 y cumplir con todos los principios y obligaciones que la normativa sobre protección de datos personales establece.

Tampoco es objeto de la presente circular el derecho de los usuarios a no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de comunicación comercial sin haber prestado su consentimiento previo para ello, previsto en el artículo 66.1.a) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

Artículo 2. *Consentimiento de los usuarios finales.*

El consentimiento de los usuarios finales deberá haber sido prestado de acuerdo con las previsiones del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018, de 5 de diciembre.

No podrán realizarse llamadas comerciales a números generados de forma aleatoria sin el consentimiento previo del usuario.

Las llamadas a los usuarios que figuren en las guías de abonados requerirán que hayan prestado su consentimiento específico previo para que sus datos puedan ser usados con fines comerciales, debiendo constar expresamente dicho consentimiento, con carácter general, en las correspondientes guías.

Artículo 3. *Interés legítimo del responsable o de terceros.*

En virtud de la remisión contenida en el artículo 66.1.b) de la Ley 11/2022, de 28 de junio, a las bases de legitimación del artículo 6.1 del Reglamento (UE) 2016/679, será lícito el tratamiento de los datos personales de los usuarios finales si es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño, de conformidad con la letra f) del citado artículo 6.1 del Reglamento (UE) 2016/679.

El responsable del tratamiento deberá realizar, con carácter previo al inicio del tratamiento y atendiendo a las distintas categorías de afectados, la correspondiente

ponderación de los derechos e intereses en conflicto. En caso de ser requerido, el responsable deberá justificar la correspondiente ponderación ante la Agencia Española de Protección de Datos y, en su caso, ante los organismos de supervisión o de resolución de controversias previstos en los códigos de conducta que sean aplicables por razón de la materia.

La AEPD presumirá, salvo prueba en contrario, que el tratamiento es lícito cuando exista una relación contractual previa, siempre que el responsable hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. Esta presunción no ampara la comunicación de los datos personales a otras entidades pertenecientes al mismo grupo empresarial con fines de comunicación comercial, siendo necesario el consentimiento específico previo del usuario.

La AEPD no presumirá en el marco de esta ponderación, salvo prueba en contrario, la existencia de expectativa razonable de los interesados en aquellos casos en los que no exista relación contractual vigente, solicitud o interacción previa y realizada durante el último año por parte del interesado con el responsable que pretenda realizar la acción comercial, particularmente cuanto este tratamiento suponga una pérdida de control del interesado sobre sus datos.

En todo caso, deberá cumplirse el deber de transparencia, conforme a los artículos 13 y 14 del Reglamento (UE) 2016/679 y facilitarse el ejercicio del derecho de oposición que será mencionado explícitamente al interesado, a más tardar, en la primera comunicación, de acuerdo con el artículo 21.4 del citado reglamento.

Artículo 4. *Consulta de los sistemas de exclusión publicitaria.*

Deberán consultarse previamente los sistemas de exclusión publicitaria, en los casos y términos previstos en el artículo 23 de la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 5. *Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.*

Se presumirá lícito el tratamiento de los datos de las personas físicas que presten servicios en una persona jurídica, empresarios individuales y profesionales liberales, en los casos y términos previstos en el artículo 19 de Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 6. *Otras garantías adicionales.*

Para el adecuado cumplimiento de los principios de lealtad y transparencia, así como del principio de responsabilidad proactiva, contemplados en el artículo 5 del Reglamento (UE) 2016/679, según el criterio de esta Agencia, deberán adoptarse garantías adicionales, entre las que se encuentran las siguientes:

a) Al inicio de cada llamada, informar sobre la identidad del empresario, y si procede, la identidad de la persona por cuenta de la cual se efectúa la llamada, indicar la finalidad comercial de la misma e informar sobre la posibilidad de revocar el consentimiento o ejercer el derecho de oposición a recibir llamadas comerciales no deseadas.

b) Cualquier manifestación inequívoca del usuario contraria a la recepción de dichas llamadas deberá entenderse como revocación del consentimiento o, en su caso, ejercicio del derecho de oposición, debiendo atenderse inmediatamente.

c) La grabación de la llamada como medio de demostrar el cumplimiento de la normativa sobre protección de datos personales.

Disposición final. *Entrada en vigor.*

La presente circular entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 28

Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos

Comunidad Autónoma de Cataluña
«DOGC» núm. 5731, de 8 de octubre de 2010
«BOE» núm. 257, de 23 de octubre de 2010
Última modificación: 13 de marzo de 2015
Referencia: BOE-A-2010-16136

EL PRESIDENTE DE LA GENERALIDAD DE CATALUÑA

Sea notorio a todos los ciudadanos que el Parlamento de Cataluña ha aprobado y yo, en nombre del Rey y de acuerdo con lo que establece el artículo 65 del Estatuto de autonomía de Cataluña, promulgo la siguiente Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.

PREÁMBULO

La recogida y el tratamiento de información por parte de las entidades que forman el sector público, necesarios para el desarrollo de las funciones que les encomienda el ordenamiento jurídico, ha experimentado en los últimos años un considerable crecimiento, derivado no solo de la ampliación de la actividad del sector público, sino, fundamentalmente, del espectacular crecimiento de las posibilidades que ofrecen los medios tecnológicos para el tratamiento de la información. En este contexto y ante los riesgos que este fenómeno comporta, adquiere una relevancia creciente el derecho a la protección de datos, no únicamente para preservar el derecho a la intimidad, sino también, con carácter instrumental, para preservar los demás derechos de la persona reconocidos por la Constitución, el Estatuto de autonomía y el resto del ordenamiento jurídico.

El derecho a la protección de datos está reconocido por el Convenio 108, de 28 de enero de 1981, del Consejo de Europa, por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, así como por el artículo 18.4 de la Constitución española y el artículo 31 del Estatuto de autonomía. Regulado en el ámbito estatal por la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, el derecho a la protección de datos comporta no solo el poder jurídico de imponer a terceros el deber de abstenerse de cualquier intromisión en la esfera íntima de la persona, sino, más allá de eso, un poder de disposición sobre los datos personales que se traduce en el reconocimiento del derecho a que se requiera el consentimiento para el uso y la recogida de dichos datos personales, del derecho a ser informado, del derecho a acceder, rectificar, cancelar dichos datos y oponerse a su utilización en determinados supuestos, así como del derecho a que la recogida y el tratamiento sean realizados en condiciones que garanticen su seguridad.

La Agencia Catalana de Protección de Datos, autoridad independiente creada por la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, ha velado por la garantía del derecho a la protección de datos en el ámbito de las administraciones públicas de Cataluña mediante el asesoramiento, la difusión del derecho y el cumplimiento de las funciones de control establecidas por el ordenamiento jurídico.

La aprobación del Estatuto de autonomía de 2006 supuso el reconocimiento expreso, por vez primera en el ámbito estatutario, del derecho a la protección de datos y reforzó el papel de la autoridad de control en materia de protección de datos, ya que, por una parte, clarificó y amplió su ámbito de actuación y, por otra, reforzó su independencia al establecer su designación parlamentaria.

Junto con estas exigencias derivadas del Estatuto de autonomía y otras mejoras técnicas necesarias, es preciso también incorporar a la legislación vigente en Cataluña otras modificaciones, como la propia denominación de la autoridad, para evitar la confusión de su naturaleza con el de las entidades de carácter instrumental que bajo la denominación de agencias han aparecido últimamente en el ámbito administrativo.

CAPÍTULO I

Disposiciones generales

Artículo 1. *La Autoridad Catalana de Protección de Datos.*

La Autoridad Catalana de Protección de Datos es el organismo independiente que tiene por objeto garantizar, en el ámbito de las competencias de la Generalidad, los derechos a la protección de datos personales y de acceso a la información vinculada a ellos.

Artículo 2. *Naturaleza jurídica.*

1. La Autoridad Catalana de Protección de Datos es una institución de derecho público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, con plena autonomía orgánica y funcional, que actúa con objetividad y plena independencia de las administraciones públicas en el ejercicio de sus funciones.

2. La Autoridad Catalana de Protección de Datos se relaciona con el Gobierno mediante el departamento que se determine por reglamento.

Artículo 3. *Ámbito de actuación.*

El ámbito de actuación de la Autoridad Catalana de Protección de Datos comprende los ficheros y los tratamientos que llevan a cabo:

a) Las instituciones públicas.

b) La Administración de la Generalidad.

c) Los entes locales.

d) Las entidades autónomas, los consorcios y las demás entidades de derecho público vinculadas a la Administración de la Generalidad o a los entes locales, o que dependen de ellos.

e) Las entidades de derecho privado que cumplan, como mínimo, uno de los tres requisitos siguientes con relación a la Generalidad, a los entes locales o a los entes que dependen de ellos:

Primero.–Que su capital pertenezca mayoritariamente a dichos entes públicos.

Segundo.–Que sus ingresos presupuestarios provengan mayoritariamente de dichos entes públicos.

Tercero.–Que en sus órganos directivos los miembros designados por dichos entes públicos sean mayoría.

f) Las demás entidades de derecho privado que prestan servicios públicos mediante cualquier forma de gestión directa o indirecta, si se trata de ficheros y tratamientos vinculados a la prestación de dichos servicios.

g) Las universidades públicas y privadas que integran el sistema universitario catalán, y los entes que de ellas dependen.

h) Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalidad o de los entes locales, si se trata de ficheros o tratamientos destinados al ejercicio de dichas funciones y el tratamiento se lleva a cabo en Cataluña.

i) Las corporaciones de derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña a los efectos de lo establecido por la presente ley.

Artículo 4. *Competencias.*

Para el cumplimiento de las funciones que la presente ley le asigna y dentro de su ámbito de actuación, corresponden a la Autoridad Catalana de Protección de Datos las competencias de registro, control, inspección, sanción y resolución, así como la aprobación de propuestas, recomendaciones e instrucciones.

Artículo 5. *Funciones.*

Las funciones de la Autoridad Catalana de Protección de Datos son:

a) Velar por el cumplimiento de la legislación vigente sobre protección de datos de carácter personal.

b) Resolver las reclamaciones de tutela formuladas por las personas afectadas respecto al ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

c) Promover, en el ámbito de sus competencias, la divulgación de los derechos de las personas con relación a la protección de datos y el acceso a la información, y la evaluación del impacto sobre la privacidad.

d) Velar por el cumplimiento de las disposiciones que la Ley 23/1998, de 30 de diciembre, de estadística de Cataluña establece respecto a la recogida de datos estadísticos y al secreto estadístico, y adoptar las medidas correspondientes para garantizar las condiciones de seguridad de los ficheros constituidos con finalidades exclusivamente estadísticas, sin perjuicio de las competencias atribuidas al Instituto de Estadística de Cataluña. A tales efectos, la Autoridad, en el ámbito de sus competencias, puede adoptar instrucciones y resoluciones dirigidas a los órganos administrativos y puede solicitar, si procede, la colaboración del Instituto de Estadística de Cataluña.

e) Dictar, sin perjuicio de las competencias de otros órganos e instituciones, las instrucciones y las recomendaciones en materia de protección de datos de carácter personal y de acceso a la información.

f) Requerir a los responsables del fichero o del tratamiento y a los encargados del tratamiento la adopción de las medidas necesarias para la adecuación del tratamiento de los datos personales objeto de investigación a la legislación vigente en materia de protección de datos de carácter personal y, en su caso, ordenar el cese de los tratamientos y la supresión de los ficheros.

g) Proporcionar información sobre los derechos de las personas en materia de tratamiento de datos personales.

h) Atender las peticiones de información, las quejas y las denuncias.

i) Decidir sobre las inscripciones de ficheros y el tratamiento de datos de carácter personal en el Registro de Protección de Datos de Cataluña, así como tener conocimiento de los demás ficheros en que, a pesar de estar exentos del deber de inscripción en el Registro, la legislación vigente establezca un deber de comunicación a la autoridad de protección de datos.

j) Ejercer la potestad de inspección.

k) Ejercer la potestad sancionadora sobre cualquier tipo de fichero o tratamiento sometido a la normativa de protección de datos, en el ámbito que establece el artículo 3.

l) Elaborar planes de auditoría.

m) Emitir informe, con carácter preceptivo, sobre los proyectos de disposiciones de carácter general de la Generalidad de creación, modificación o supresión de ficheros de datos de carácter personal, y sobre las disposiciones que afecten a la protección de datos de carácter personal.

n) Emitir informe, con carácter potestativo, sobre los proyectos de disposiciones de carácter general de los entes locales de creación, modificación o supresión de ficheros, y

sobre las disposiciones que tengan impacto en materia de protección de datos de carácter personal que los entes locales le sometan.

o) Responder a las consultas que formulen las entidades de su ámbito de actuación sobre la protección de datos de carácter personal al poder de las administraciones públicas y colaborar con estas entidades en la difusión de las obligaciones derivadas de la legislación reguladora de estas materias.

p) Otorgar las autorizaciones para la exención del deber de información en la recogida de datos, para el mantenimiento íntegro de determinados datos y las demás autorizaciones que establece la normativa vigente en materia de protección de datos.

q) Colaborar con la Agencia Española de Protección de Datos y con las demás agencias autonómicas, de acuerdo con lo establecido por la normativa reguladora de la agencia estatal.

r) Cumplir las demás funciones que le sean atribuidas de acuerdo con las leyes.

CAPÍTULO II

Organización

Artículo 6. *Órganos de gobierno.*

Los órganos de la Autoridad Catalana de Protección de Datos son:

a) El director o directora.

b) El Consejo Asesor de Protección de Datos.

Artículo 7. *El director o directora.*

1. El director o directora de la Autoridad Catalana de Protección de Datos dirige la institución y ejerce su representación.

2. El director o directora de la Autoridad Catalana de Protección de Datos, con sujeción al ordenamiento jurídico, con plena independencia y objetividad y sin sujeción a mandato imperativo alguno ni a instrucción de ninguna clase, ejerce las funciones que establece el artículo 8 y las que se establezcan por ley o reglamento.

3. El director o directora de la Autoridad Catalana de Protección de Datos es designado por el Pleno del Parlamento por mayoría de tres quintas partes, a propuesta del Consejo Asesor de Protección de Datos, de entre personas con condición política de catalanes, con pleno uso de sus derechos civiles y políticos y con experiencia en materia de protección de datos. Si no obtiene la mayoría requerida, debe someterse a una segunda votación, en la misma sesión del Pleno, en que requiere el voto favorable de la mayoría absoluta de los miembros de la cámara.

4. Los candidatos a director o directora de la Autoridad Catalana de Protección de Datos que proponga el Consejo Asesor de Protección de Datos deben comparecer ante la correspondiente comisión del Parlamento de Cataluña para que sus miembros puedan pedir las pertinentes aclaraciones y explicaciones sobre cualquier aspecto relacionado con su formación académica, trayectoria profesional o méritos alegados.

5. El director o directora de la Autoridad Catalana de Protección de Datos es elegido por un periodo de cinco años, renovable una sola vez.

6. El director o directora de la Autoridad Catalana de Protección de Datos cesa por las siguientes causas:

a) Por expiración del plazo del mandato.

b) A petición propia.

c) Por separación, acordada por el Pleno del Parlamento por mayoría de tres quintas partes, por incumplimiento grave de sus obligaciones, incompatibilidad, incapacidad sobrevenida para el ejercicio de sus funciones declarada por sentencia firme o condena firme por delito doloso.

7. El director o directora de la Autoridad Catalana de Protección de Datos tiene la consideración de alto cargo, asimilado al de secretario o secretaria general. El cargo, sin

perjuicio del régimen de incompatibilidades de los altos cargos al servicio de la Generalidad, es incompatible con:

a) El ejercicio de cualquier mandato representativo.

b) El ejercicio de funciones directivas o ejecutivas en partidos políticos, sindicatos o asociaciones empresariales, o el estar afiliado a ellos.

c) La pertenencia al Consejo de Garantías Estatutarias o al Tribunal Constitucional.

d) El ejercicio de cualquier cargo político o función administrativa en organismos internacionales, la Unión Europea, el Estado, las comunidades autónomas o las entidades locales.

e) El ejercicio de las carreras judicial, fiscal o militar.

f) El desarrollo de cualquier actividad profesional, mercantil, industrial o laboral.

Artículo 8. *Funciones del director o directora.*

1. Corresponde al director o directora de la Autoridad Catalana de Protección de Datos dictar las resoluciones y las instrucciones y aprobar las recomendaciones y los dictámenes que requiera el ejercicio de las funciones de la Autoridad, y en especial aprobar las instrucciones a que se refiere el artículo 15.

2. Corresponden al director o directora de la Autoridad Catalana de Protección de Datos, en el ámbito específico de las competencias de la Autoridad, las siguientes funciones:

a) Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones que deban practicarse en el Registro de Protección de Datos de Cataluña.

b) Resolver motivadamente sobre la procedencia o improcedencia de la denegación del ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

c) Requerir a los responsables y a los encargados del tratamiento la adopción de las medidas necesarias para la adecuación del tratamiento de datos personales objeto de investigación a la legislación vigente y ordenar, si procede, el cese de los tratamientos y la cancelación de los ficheros.

d) Adoptar las medidas, resoluciones e instrucciones necesarias para garantizar las condiciones de seguridad de los ficheros constituidos con finalidades exclusivamente estadísticas.

e) Dictar las instrucciones y recomendaciones necesarias para adecuar los tratamientos de datos personales a los principios de la legislación vigente en materia de datos personales.

f) Emitir informe, con carácter preceptivo, de los anteproyectos de ley, de los proyectos de disposiciones normativas que elabore el Gobierno por delegación legislativa y de los proyectos de reglamentos o disposiciones de carácter general que afecten a la protección de datos de carácter personal.

g) Responder a las consultas que la Administración de la Generalidad, los entes locales y las universidades de Cataluña le formulen sobre la aplicación de la legislación de protección de datos de carácter personal.

h) Resolver sobre la adopción de medidas para corregir los efectos de las infracciones.

i) Proponer el inicio de actuaciones disciplinarias contra los responsables o los encargados del tratamiento, de acuerdo con lo establecido por la legislación vigente sobre régimen disciplinario de las administraciones públicas.

j) Resolver los expedientes sancionadores que sean de su competencia y poner en conocimiento de la Agencia Española de Protección de Datos las presuntas infracciones cuya sanción le corresponda.

k) Ordenar el cese del tratamiento, de la comunicación ilícita de datos o la inmovilización de los ficheros, cuando proceda.

l) Proporcionar información sobre los derechos de las personas en materia de tratamiento de datos personales.

m) Cumplir las funciones con relación a los planes de auditoría de la Autoridad a que se refiere el artículo 20.

n) Atender las peticiones que le formulen los ciudadanos.

o) Responder a las consultas que le formulen las administraciones.

p) Elaborar la memoria anual de las actuaciones y actividades de la Autoridad a que se refiere el artículo 13 y comparecer ante la comisión pertinente del Parlamento para informar de su contenido.

q) Cumplir cualquier otra que le sea encomendada por ley o reglamento.

3. Corresponden al director o directora de la Autoridad Catalana de Protección de Datos, en los ámbitos económico, de contratación y de recursos humanos de la Autoridad, las siguientes funciones:

a) Adjudicar y formalizar los contratos que requiera la gestión de la Autoridad y vigilar su cumplimiento y ejecución.

b) Aprobar los gastos y ordenar los pagos, dentro de los límites de los créditos del presupuesto de gastos de la Autoridad.

c) Elaborar el anteproyecto de presupuesto de la Autoridad y someterlo a la consideración del Consejo Asesor de Protección de Datos.

d) Aprobar la plantilla de personal de la Autoridad.

Artículo 9. *El Consejo Asesor de Protección de Datos.*

1. El Consejo Asesor de Protección de Datos es el órgano de asesoramiento y participación de la Autoridad Catalana de Protección de Datos y está constituido por los siguientes miembros:

a) El presidente o presidenta, que es nombrado por el Consejo de entre sus miembros, una vez efectuada la renovación ordinaria de los miembros designados por el Parlamento.

b) Tres personas designadas por el Parlamento, por mayoría de tres quintas partes. Si no obtienen la mayoría requerida, deben someterse a una segunda votación, en la misma sesión del Pleno, en que se requiere el voto favorable de la mayoría absoluta.

c) Tres personas en representación de la Administración de la Generalidad, designadas por el Gobierno.

d) Dos personas en representación de la Administración local de Cataluña, designadas por el Consejo de Gobiernos Locales.

e) Una persona experta en el ámbito de los derechos fundamentales, designada por el Consejo Interuniversitario de Cataluña.

f) Una persona experta en informática, designada por el Consejo Interuniversitario de Cataluña.

g) Una persona designada por el Instituto de Estudios Catalanes.

h) Una persona en representación de las organizaciones de consumidores y usuarios, designada por el Consejo de las Personas Consumidoras de Cataluña.

i) El director o directora del Instituto de Estadística de Cataluña.

j) Un funcionario o funcionaria de la Autoridad Catalana de Protección de Datos, que actúa de secretario o secretaria del Consejo.

2. La renovación de los miembros del Consejo Asesor de Protección de Datos se lleva a cabo cada cinco años de acuerdo con los estatutos de la Autoridad Catalana de Protección de Datos.

3. El director o directora de la Autoridad Catalana de Protección de Datos asiste a las reuniones del Consejo Asesor de Protección de Datos con voz y sin voto.

Artículo 10. *Funciones del Consejo Asesor de Protección de Datos.*

1. Las funciones del Consejo Asesor de Protección de Datos son:

a) Proponer al Parlamento la persona o personas candidatas a ocupar el puesto de director o directora de la Autoridad.

b) Emitir informe sobre los proyectos de instrucciones de la Autoridad que le sean sometidos.

c) Emitir informe sobre el anteproyecto de presupuesto anual de la Autoridad que el director o directora proponga.

d) Asesorar al director o directora de la Autoridad sobre cuantas cuestiones le sean sometidas.

e) Elaborar un informe preceptivo previo a la aprobación de la plantilla del personal de la Autoridad.

f) Elaborar un informe vinculante sobre el número máximo de trabajadores de la plantilla de personal eventual de la Autoridad.

g) Elaborar estudios y propuestas en materia de protección de datos de carácter personal y pedir al director o directora el establecimiento de criterios en la materia.

2. El Consejo Asesor de Protección de Datos ha de ser informado de:

a) La actividad de la Autoridad Catalana de Protección de Datos, por parte del director o directora y de forma periódica.

b) La memoria anual de la Autoridad.

c) Los criterios objetivos de los planes de auditoría a que se refiere el artículo 20.

3. El Consejo Asesor de Protección de Datos se rige por las normas que se establezcan por reglamento y, supletoriamente, por las disposiciones vigentes sobre funcionamiento de órganos colegiados de la Administración de la Generalidad.

Artículo 11. *El Registro de Protección de Datos de Cataluña.*

1. El Registro de Protección de Datos de Cataluña se integra en la Autoridad Catalana de Protección de Datos.

2. Son objeto de inscripción en el Registro de Protección de Datos de Cataluña:

a) Los ficheros de datos personales, de titularidad pública o privada, incluidos dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos.

b) Los códigos tipo formulados por las entidades incluidas dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos.

c) Las autorizaciones de tratamientos de datos de carácter personal previstas en la legislación vigente.

3. El Gobierno debe establecer por reglamento el procedimiento de inscripción de la creación, la modificación y la supresión de ficheros en el Registro de Protección de Datos de Cataluña, así como el contenido de los asientos registrales.

4. El Registro de Protección de Datos de Cataluña es de consulta pública y gratuita. Cualquier persona puede consultar, como mínimo, la información sobre la existencia de un determinado tratamiento de datos de carácter personal, las finalidades y la identidad de la persona responsable del tratamiento.

5. La Autoridad Catalana de Protección de Datos debe establecer los acuerdos de cooperación necesarios con la Agencia Española de Protección de Datos para integrar la información registral y mantenerla actualizada.

CAPÍTULO III

Relaciones con otros organismos e instituciones

Artículo 12. *Colaboración con otras instituciones.*

La Autoridad Catalana de Protección de Datos puede suscribir convenios de colaboración con el Síndic de Greuges, los síndicos locales, el Instituto de Estadística de Cataluña, las universidades y otras instituciones y organismos de defensa de los derechos de las personas.

Artículo 13. *Memoria anual.*

1. La Autoridad Catalana de Protección de Datos debe elaborar una memoria anual de sus actividades y de las conclusiones de los trabajos y expedientes que ha tramitado.

2. La Autoridad Catalana de Protección de Datos debe presentar la memoria anual en el Parlamento y dar cuenta de la misma en el marco de la comisión correspondiente, y remitirla también al Gobierno, al Síndic de Greuges y al director o directora de la Agencia Española de Protección de Datos.

Artículo 14. *Relaciones entre la Autoridad Catalana de Protección de Datos y el Síndic de Greuges.*

Las relaciones entre la Autoridad Catalana de Protección de Datos y el Síndic de Greuges son de colaboración en el ámbito de sus respectivas competencias.

CAPÍTULO IV

Ejercicio de competencias y funciones

Artículo 15. *Instrucciones.*

1. El director o directora de la Autoridad Catalana de Protección de Datos puede aprobar instrucciones para la adecuación de los ficheros y los tratamientos de datos a los principios y garantías que establece la legislación vigente en materia de protección de datos.
2. El proyecto de instrucción debe someterse a información pública y a informe del Consejo Asesor de Protección de Datos. Igualmente, puede ser sometido a informe de la Comisión Jurídica Asesora.
3. Las instrucciones a que se refiere el apartado 1 se publican en el «Diari Oficial de la Generalitat de Catalunya» y en la sede electrónica de la Autoridad Catalana de Protección de Datos.

Artículo 16. *Tutela de los derechos de acceso, rectificación, oposición y cancelación.*

1. Las personas interesadas a las que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, de rectificación, de cancelación o de oposición, o que puedan entender desestimada su solicitud por el hecho de no haber sido resuelta y remitida dentro del plazo establecido, pueden presentar una reclamación ante la Autoridad Catalana de Protección de Datos.
2. La Autoridad Catalana de Protección de Datos debe resolver expresamente sobre la procedencia o improcedencia de la reclamación a que se refiere el apartado 1 en el plazo de seis meses, previa audiencia de la persona responsable del fichero así como de las personas interesadas si el resultado del primer trámite de audiencia lo hace necesario. Transcurrido dicho plazo sin que la Autoridad notifique la resolución, se entiende que ha sido desestimada.
3. La resolución de estimación total o parcial de la tutela de un derecho ha de establecer el plazo en que este debe hacerse efectivo.
4. Si la solicitud de ejercicio del derecho ante la persona responsable del fichero es estimada, total o parcialmente, pero el derecho no se ha hecho efectivo en la forma y los plazos exigibles de acuerdo con la normativa aplicable, las personas interesadas pueden ponerlo en conocimiento de la Autoridad Catalana de Protección de Datos para que se lleven a cabo las correspondientes actuaciones sancionadoras.

Artículo 17. *Publicidad de los informes y resoluciones.*

1. La Autoridad Catalana de Protección de Datos está obligada a garantizar la confidencialidad de las consultas y reclamaciones de que tenga conocimiento, sin perjuicio del derecho de acceso a la información y documentación administrativas de las personas interesadas.
2. Los dictámenes, informes y resoluciones de la Autoridad Catalana de Protección de Datos deben hacerse públicos, una vez notificados a las personas interesadas, previa «anonimización» de los datos de carácter personal, sin perjuicio de lo establecido por el apartado 1.
3. De forma excepcional, puede optarse por no publicar las resoluciones sin interés doctrinal alguno o que, pese a la «anonimización», sea aconsejable por causas justificadas evitar su publicidad para impedir hacer reconocibles a las personas que lo solicitan.

Artículo 18. *Funciones de control.*

1. La actividad de control de la Autoridad Catalana de Protección de Datos se lleva a cabo mediante la potestad de inspección, los planes de auditoría, la aplicación del régimen sancionador, los requerimientos de adecuación a la legalidad y la potestad de inmovilización de ficheros.

2. Los hechos constatados por los funcionarios al servicio de la Autoridad Catalana de Protección de Datos al llevar a cabo su tarea de control e inspección, si sus actuaciones se formalizan en un documento público en que se observen los requisitos legales pertinentes, tienen valor probatorio, sin perjuicio de las pruebas en defensa de los respectivos derechos o intereses que puedan aportar los propios interesados.

Artículo 19. *Potestad de inspección.*

1. La Autoridad Catalana de Protección de Datos puede inspeccionar los ficheros y los tratamientos de datos personales a que se refiere la presente ley, a fin de obtener todas las informaciones necesarias para el ejercicio de sus funciones. A tal fin, la Autoridad puede solicitar la presentación o la remisión de documentos y de datos o examinarlos en el lugar donde estén depositados, así como inspeccionar los equipos físicos y lógicos utilizados, para lo cual puede acceder a los locales donde estén instalados.

2. Los funcionarios que ejercen la función inspectora a que se refiere el apartado 1 tienen la consideración de autoridad pública en el desarrollo de su actividad y quedan obligados a mantener el secreto sobre las informaciones que conozcan en el ejercicio de las funciones inspectoras, incluso después de haber cesado en las mismas.

3. En el ejercicio de las funciones de inspección los funcionarios pueden ser auxiliados por personal no funcionario, si así lo decide el director o directora de la Autoridad, en función de los conocimientos de orden técnico que puedan ser necesarios para auditar sistemas de información durante las tareas de investigación. El personal no funcionario que participa en la actividad inspectora debe hacerlo siguiendo las instrucciones y bajo la supervisión del personal funcionario inspector, y tiene las mismas obligaciones que este, especialmente en cuanto al deber de secreto.

4. Las entidades comprendidas dentro del ámbito de aplicación de la presente ley tienen la obligación de auxiliar, con carácter preferente y urgente, a la Autoridad Catalana de Protección de Datos en sus investigaciones, si esta lo solicita.

Artículo 20. *Planes de auditoría.*

1. Los planes de auditoría de la Autoridad Catalana de Protección de Datos constituyen un sistema de control preventivo para:

a) Verificar el cumplimiento de la normativa en materia de protección de datos de carácter personal.

b) Recomendar o requerir a los responsables de los ficheros y de los tratamientos de datos de carácter personal la adopción de las medidas correctoras adecuadas.

2. Corresponde al director o directora de la Autoridad Catalana de Protección de Datos:

a) Decidir el contenido de cada plan de auditoría y concretar los aspectos y tratamientos que deben ser analizados.

b) Seleccionar las entidades que deben ser objeto de los planes de auditoría mediante criterios objetivos que han de ser públicos.

3. Las entidades a que se refiere la letra b del apartado 2 deben colaborar con la persona responsable de la auditoría facilitando la realización de las verificaciones oportunas y aportando la información y documentación necesarias.

4. Las conclusiones de los planes de auditoría sobre el grado general de cumplimiento y las recomendaciones generales pertinentes deben difundirse públicamente.

5. Si durante el proceso de ejecución de un plan de auditoría la entidad afectada es objeto, previa denuncia, de la incoación de un expediente sancionador por parte de la Autoridad Catalana de Protección de Datos como consecuencia de la comisión de una posible infracción por algún aspecto coincidente o directamente relacionado con el contenido

del plan de auditoría que se está llevando a cabo, la entidad debe ser excluida del plan de auditoría y debe continuarse la tramitación del procedimiento sancionador.

6. Los requerimientos a que se refiere la letra b del apartado 1 deben establecer un plazo adecuado para la adopción de las medidas correctoras necesarias por parte de las entidades afectadas. Transcurrido dicho plazo sin que la entidad afectada informe a la Autoridad Catalana de Protección de Datos sobre las medidas adoptadas, o si estas son insuficientes o inadecuadas, la Autoridad puede iniciar las actuaciones inspectoras oportunas para incoar, si procede, un procedimiento sancionador.

Artículo 21. *Régimen sancionador.*

1. Los responsables de los ficheros y de los tratamientos de datos personales incluidos dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos y los encargados de los correspondientes tratamientos quedan sujetos al régimen sancionador establecido por la legislación estatal de protección de datos de carácter personal. Las referencias a la Agencia Española de Protección de Datos o a sus órganos, en cuanto al régimen de infracciones, deben entenderse hechas a la Autoridad Catalana de Protección de Datos o a sus órganos, en lo concerniente a su ámbito competencial.

2. En el caso de infracciones cometidas con relación a ficheros de titularidad pública, el director o directora de la Autoridad Catalana de Protección de Datos debe dictar una resolución que declare la infracción y establezca las medidas a adoptar para corregir sus efectos. Además, puede proponer, si procede, la iniciación de actuaciones disciplinarias de acuerdo con lo establecido por la legislación vigente sobre el régimen disciplinario del personal al servicio de las administraciones públicas. Dicha resolución debe notificarse a la persona responsable del fichero o del tratamiento, a la encargada del tratamiento, si procede, al órgano del que dependan y a las personas afectadas, si las hay.

3. En el caso de infracciones cometidas con relación a ficheros de titularidad privada, la resolución que declare la infracción debe imponer las sanciones previstas por la legislación de protección de datos y las medidas a adoptar para corregir los efectos de la infracción.

4. El director o directora de la Autoridad Catalana de Protección de Datos debe informar al síndic o síndica de greuges de las actuaciones que haga a consecuencia de una solicitud del mismo y debe comunicarle las resoluciones sancionadoras que dicte con relación a dichas actuaciones.

Artículo 22. *Procedimiento sancionador.*

1. El Gobierno debe establecer por decreto el procedimiento para la determinación de las infracciones y la imposición de sanciones.

2. La denuncia que inicia un procedimiento sancionador debe formalizarse mediante escrito razonado y estar debidamente firmada.

3. La persona denunciante debe identificarse en el momento de hacer la denuncia a que se refiere el apartado 2. Sin embargo, puede solicitar de forma razonada que su identidad no sea revelada, previa ponderación de los intereses en conflicto por la Autoridad Catalana de Protección de Datos, cuando haya motivos fundamentados y legítimos relativos a una situación personal concreta que así lo justifique.

4. La persona denunciante tiene derecho a que le sean comunicadas las actuaciones que se deriven de su denuncia, sin perjuicio de los derechos que puedan corresponderle si también es persona interesada.

Artículo 23. *Medidas provisionales.*

En el momento de la incoación o durante la tramitación del procedimiento sancionador, el director o directora de la Autoridad Catalana de Protección de Datos puede adoptar, de forma motivada, las medidas provisionales que considere necesarias para asegurar la eficacia de la resolución que finalmente pueda recaer y para conseguir la protección provisional del derecho a la protección de datos de las personas afectadas. Con carácter previo, la Autoridad debe dar audiencia a las entidades afectadas, excepto si concurren circunstancias de urgencia que puedan hacer perder la finalidad de la medida. La resolución que adopte la medida es susceptible de los recursos procedentes.

Artículo 24. *Cumplimiento de la resolución del procedimiento sancionador.*

1. En las infracciones declaradas respecto a ficheros de titularidad pública, las personas o entidades que hayan sido declaradas responsables de la infracción deben comunicar a la Autoridad Catalana de Protección de Datos, en el plazo que establece la resolución, la adopción de las medidas y actuaciones a que se refiere el apartado 2 del artículo 25.

2. En las sanciones impuestas por infracciones cometidas respecto a ficheros de titularidad privada, el cumplimiento de la sanción debe llevarse a cabo en el plazo establecido por la legislación vigente. Dentro de este plazo, la entidad sancionada puede solicitar, de forma razonada, el fraccionamiento del pago. El director o directora de la Autoridad Catalana de Protección de Datos debe resolver la solicitud, de acuerdo con lo establecido por la normativa reguladora de la recaudación de los ingresos públicos.

3. Las personas o entidades sancionadas a quienes se haya impuesto alguna medida correctora de acuerdo con lo establecido por el artículo 25 deben comunicar a la Autoridad Catalana de Protección de Datos, en el plazo que establece la resolución, las medidas adoptadas.

Artículo 25. *Requerimientos de adecuación y potestad de inmovilización.*

1. En los supuestos, constitutivos de infracción muy grave, de utilización o de comunicación ilícita de datos personales en que se atente gravemente contra los derechos fundamentales y las libertades públicas de los ciudadanos o se impida su ejercicio, el director o directora de la Autoridad Catalana de Protección de Datos puede exigir a los responsables de los ficheros de datos personales el cese de la utilización o comunicación ilícita de datos personales.

2. Si el requerimiento a que se refiere el apartado 1 no es atendido, el director o directora de la Autoridad Catalana de Protección de Datos puede, mediante resolución motivada, inmovilizar los ficheros de datos personales, con la única finalidad de restaurar los derechos de las personas afectadas. En este supuesto, la inmovilización queda sin efecto de no acordar la Autoridad, en el plazo de quince días, la incoación de un procedimiento sancionador y ratificarse la medida.

CAPÍTULO V

Régimen jurídico, de personal, económico y de contratación

Artículo 26. *Régimen jurídico.*

1. La Autoridad Catalana de Protección de Datos, en el ejercicio de sus funciones, actúa de conformidad con lo dispuesto por la presente ley, sus disposiciones de desarrollo y la legislación reguladora del régimen jurídico de las administraciones públicas y el procedimiento administrativo aplicable a la Administración de la Generalidad.

2. Las resoluciones del director o directora de la Autoridad Catalana de Protección de Datos agotan la vía administrativa y son susceptibles de recurso contencioso-administrativo, sin perjuicio de los recursos administrativos que procedan.

Artículo 27. *Régimen de personal.*

1. La Autoridad Catalana de Protección de Datos, en el ejercicio de su potestad de autoorganización y de acuerdo con los créditos consignados en los presupuestos de la Generalidad, aprueba la relación de puestos de trabajo de los órganos y servicios que la integran y que han de ser ocupados por personal funcionario, laboral o eventual, e informa de ello al Parlamento.

2. Al personal al servicio de la Autoridad Catalana de Protección de Datos se le aplica a todos los efectos la normativa que regula el estatuto del personal al servicio de la Administración de la Generalidad en cuanto al régimen y la normativa de ordenación de la ocupación pública.

3. Los puestos de trabajo que comportan el ejercicio de potestades públicas se reservan a personal funcionario.

4. Los puestos de trabajo considerados de confianza o de asesoramiento especial no reservado a personal funcionario y que figuran con este carácter en la correspondiente relación de puestos de trabajo son desempeñados por personal eventual, cuyo número máximo fija el Consejo Asesor de Protección de Datos.

5. La Autoridad Catalana de Protección de Datos ejerce la potestad disciplinaria respecto al personal al servicio de la institución.

6. El personal al servicio de la Autoridad Catalana de Protección de Datos tiene el deber de secreto sobre las informaciones que conozca en el ejercicio de sus funciones, incluso después de haber cesado en su ejercicio.

Artículo 28. *Régimen económico y de contratación.*

1. Para el cumplimiento de sus finalidades, la Autoridad Catalana de Protección de Datos cuenta con los siguientes bienes y recursos económicos:

a) Las asignaciones anuales de los presupuestos de la Generalidad.

b) Los bienes y derechos que constituyen su patrimonio, así como los productos y rentas de los mismos.

c) El producto de las sanciones que imponga en el ejercicio de sus competencias.

d) El producto de las tasas y demás ingresos públicos devengados por su actividad.

e) Cualquier otro recurso económico que legalmente se le pueda atribuir.

2. **(Derogado).**

3. La Autoridad Catalana de Protección de Datos debe elaborar su propuesta de anteproyecto de presupuesto de ingresos y de gastos de acuerdo con las normas que dicte el departamento competente en materia de economía y finanzas para elaborar los presupuestos de la Generalidad, y debe remitirlo al departamento mediante el que se relaciona con el Gobierno para que este, sobre la base de esta propuesta, formule el anteproyecto y tramite su inclusión en el proyecto de ley de presupuestos de la Generalidad.

4. La Autoridad Catalana de Protección de Datos está sometida al control financiero de la Intervención General de la Generalidad y al régimen de contabilidad pública.

5. El régimen jurídico de contratación de la Autoridad Catalana de Protección de Datos es el establecido por la legislación sobre contratos del sector público.

6. El régimen patrimonial de la Autoridad Catalana de Protección de Datos es el establecido por la normativa que regula el patrimonio de la Administración de la Generalidad.

Disposición transitoria primera. *Sucesión de la Agencia Catalana de Protección de Datos.*

1. La Autoridad Catalana de Protección de Datos se subroga en la posición jurídica de la Agencia Catalana de Protección de Datos en cuanto a los bienes, derechos y obligaciones de cualquier tipo de que fuera titular la Agencia.

2. Las referencias hechas en el ordenamiento jurídico a la Agencia Catalana de Protección de Datos deben entenderse hechas a la Autoridad Catalana de Protección de Datos.

Disposición transitoria segunda. *Procedimiento sancionador.*

Mientras el Gobierno no apruebe el decreto que regula el procedimiento sancionador en materia de protección de datos, continúa siendo aplicable el procedimiento establecido por el Decreto 278/1993, de 9 de noviembre, sobre procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad.

Disposición transitoria tercera. *Vigencia del Estatuto de la Agencia Catalana de Protección de Datos.*

Mientras no entren en vigor los estatutos de la Autoridad Catalana de Protección de Datos, sigue siendo de aplicación, en todo lo que no se oponga a la presente ley, el Estatuto de la Agencia Catalana de Protección de Datos, aprobado por el Decreto 48/2003, de 20 de febrero.

Disposición derogatoria.

Queda derogada la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.

Disposición final primera. *Estatutos de la Autoridad.*

En el plazo de seis meses a contar desde la entrada en vigor de la presente ley, el Gobierno debe aprobar los estatutos de la Autoridad Catalana de Protección de Datos.

Disposición final segunda. *Desarrollo de los procedimientos.*

Se habilita al Gobierno para la regulación de los procedimientos necesarios para el ejercicio de las funciones atribuidas a la Autoridad Catalana de Protección de Datos, sin perjuicio de la competencia de la Autoridad para concretar mediante instrucción aquellos aspectos en que sea necesario.

Disposición final tercera. *Creación, modificación y supresión de ficheros.*

1. Los consejeros de la Generalidad, dentro del ámbito de sus respectivas competencias, quedan habilitados para crear, modificar y suprimir, mediante orden, los ficheros de sus departamentos o de los entes públicos vinculados a ellos o que dependan de los mismos y los ficheros de los consorcios en que la representación de la Administración de la Generalidad en los órganos de gobierno sea mayoritaria.

2. Las entidades de derecho público dotadas de especial independencia o autonomía quedan habilitadas para ejercer la competencia de crear, modificar y suprimir ficheros.

§ 29

Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía

Comunidad Autónoma de Andalucía
«BOJA» núm. 124, de 30 de junio de 2014
«BOE» núm. 172, de 16 de julio de 2014
Última modificación: 4 de junio de 2024
Referencia: BOE-A-2014-7534

LA PRESIDENTA DE LA JUNTA DE ANDALUCÍA

A todos los que la presente vieren, sabed:

Que el Parlamento de Andalucía ha aprobado y yo, en nombre del Rey y por la autoridad que me confieren la Constitución y el Estatuto de Autonomía, promulgo y ordeno la publicación de la siguiente Ley de Transparencia Pública de Andalucía

EXPOSICIÓN DE MOTIVOS

I

La transparencia es inherente a la democracia y constituye una pieza fundamental para el establecimiento de una sociedad democrática avanzada, que es uno de los objetivos proclamados en el preámbulo de nuestra carta magna.

Sin el conocimiento que proporciona el acceso de los ciudadanos a la información pública, difícilmente podría realizarse la formación de la opinión crítica y la participación de todos los ciudadanos en la vida política, económica, cultural y social, un objetivo irrenunciable que los poderes públicos están obligados a fomentar (artículos 9.2 de la Constitución y 10.1 del Estatuto de Autonomía para Andalucía).

También la evaluación de programas y políticas públicas se reconoce como un instrumento operativo para cumplir objetivos de transparencia. Así, la Junta de Andalucía se marca como objetivo avanzar en el diseño de un sistema andaluz de evaluación de políticas públicas, conforme al artículo 138 del Estatuto de Autonomía y en orden a la mayor transparencia en la gestión pública.

La presente ley tiene por objeto profundizar en la transparencia de la actuación de los poderes públicos, entendida como uno de los instrumentos que permiten que la democracia sea más real y efectiva. Esta no debe quedar reducida al mero ejercicio periódico del derecho de sufragio activo. Nuestro ordenamiento jurídico exige que se profundice en la articulación de los mecanismos que posibiliten el conocimiento por la ciudadanía de la actuación de los poderes públicos, de los motivos de dicha actuación, del resultado del mismo y de la valoración que todo ello merezca.

II

Como indica el preámbulo del Convenio del Consejo de Europa sobre Acceso a los Documentos Públicos, en una sociedad democrática y pluralista, la transparencia es un requisito extremadamente importante. Por ello el ejercicio del derecho de acceso a los documentos públicos proporciona una fuente de información para el público; ayuda a este a formarse una opinión sobre el estado de la sociedad y sobre las autoridades públicas, y fomenta la integridad, la eficacia, la eficiencia y la responsabilidad de las autoridades públicas, ayudando así a que se afirme su legitimidad.

La transparencia de la actuación de los poderes públicos se articula en la presente ley a través de dos grandes conceptos, como son la publicidad activa y el acceso a la información pública.

Estos dos conceptos responden a dinámicas diferentes. La publicidad activa implica la difusión por propia iniciativa de la información que obra en poder de los poderes públicos. Se trata de posibilitar que la ciudadanía conozca la información que sea relevante para garantizar la transparencia de su actividad, implicando una actitud proactiva de los mismos.

Esta publicidad activa de la información pública supone la puesta a disposición de la ciudadanía de información atinente no sólo a los aspectos institucionales y organizativos, sino también a aspectos muy variados de la actuación pública, tales como la producción normativa, la planificación, la contratación y gestión de subvenciones o la información económica y presupuestaria, entre otros aspectos.

En el acceso a la información pública es la ciudadanía la que toma la iniciativa, recabando de los poderes públicos información que obra en su poder. Este acceso se configura como un verdadero derecho, que en su vertiente procedimental lleva a establecer la regla general del acceso a dicha información. Constituye pues la excepción la denegación o limitación del acceso. Para garantizar que esa limitación o denegación responda a verdaderas razones, así como para facilitar el control por el órgano al que se presenta la reclamación o por los tribunales de la decisión adoptada, se impone el deber de motivar dichas resoluciones.

III

Las nuevas tecnologías, por otro lado, coadyuvan a hacer posible la transparencia. En efecto, Internet se revela como un instrumento fundamental para la difusión de la información, que está produciendo la aparición de una nueva cultura en la que cada vez más personas se interrelacionan.

La red progresivamente se está convirtiendo en un lugar de encuentro, de interrelación y, por qué no decirlo, de transmisión de ideas, opiniones e información a modo de una moderna ágora virtual que nos reconduce al origen de la democracia.

La presente ley trata de aprovechar toda la potencialidad que nos ofrecen las nuevas tecnologías para servir de instrumento para la difusión de la información pública y para permitir que esa información se difunda y pueda ser utilizada por la ciudadanía, que es, como se ha dicho en alguna ocasión, la legítima propietaria de la información pública.

IV

El derecho a la información cuenta con antecedentes en el Derecho comparado. Desde la Ley de Suecia de 1766, pasando por el artículo 14 de la Declaración de Derechos Humanos y Civiles de Francia de 1789, la Resolución de la Asamblea General de la ONU, núm. 59, de 1946; la Ley de Libertad de Información de 1966 de los Estados Unidos; la Recomendación del Consejo de Europa de 1981 sobre el Acceso a la Información en manos de las Autoridades Públicas, y, finalmente, el Convenio del Consejo de Europa sobre Acceso a los Documentos Públicos de 18 de junio de 2009.

En nuestro país, tanto la Constitución española como el Estatuto de Autonomía para Andalucía cuentan con diferentes preceptos que fundamentan la regulación de la transparencia.

En desarrollo de la Constitución española, se pretende ampliar y reforzar la transparencia de la actividad pública, así como reconocer y garantizar el derecho de acceso a la información relativa a aquella actividad, con el fin de facilitar, en cumplimiento del

artículo 9.2 de la Constitución española, la participación de todos los ciudadanos en la vida política; garantizar, de conformidad con el artículo 9.3 de la Constitución española, la publicidad de las normas, la seguridad jurídica y la interdicción de la arbitrariedad de los poderes públicos; y por último, garantizar, conforme al artículo 20.1.d) de la Constitución española, el derecho a recibir libremente información veraz de los poderes públicos y, conforme al artículo 105.b) de la Constitución española, el acceso de los ciudadanos a la información pública.

Igualmente, el fomento de la transparencia encuentra fundamento en diversos preceptos del Estatuto de Autonomía para Andalucía. Pretende fomentar, de conformidad con lo dispuesto en el artículo 10.1, la calidad de la democracia facilitando la participación de todas las personas andaluzas en la vida política; conseguir, como objetivo básico, en defensa del interés general, la participación ciudadana en la elaboración, prestación y evaluación de las políticas públicas, así como la participación individual y asociada en el ámbito político, en aras de una democracia social avanzada y participativa, como dispone el artículo 10.3.19.º; promover, de conformidad con lo dispuesto en el artículo 11, el desarrollo de una conciencia ciudadana y democrática plena; constituir, de acuerdo con lo dispuesto en el artículo 30.1.e), cauce de ejercicio del derecho de participación política, y, en particular, del derecho a participar activamente en la vida pública andaluza estableciendo mecanismos necesarios de información, comunicación y recepción de propuestas.

Mención especial merece la relación de la transparencia con el derecho a una buena administración reconocido en el artículo 31, que comprende el derecho de todos ante las administraciones públicas, cuya actuación será proporcionada a sus fines, a participar plenamente en las decisiones que les afecten, obteniendo de ellas una información veraz, y a que sus asuntos se traten de manera objetiva e imparcial y sean resueltos en un plazo razonable, así como a acceder a los archivos y registros de las instituciones, corporaciones, órganos y organismos públicos de Andalucía, cualquiera que sea su soporte, con las excepciones que la ley establezca; desarrollar, de conformidad con el artículo 34, el derecho a acceder y usar las nuevas tecnologías y a participar activamente en la sociedad del conocimiento, la información y la comunicación, mediante los medios y recursos que la ley establezca; desarrollar los instrumentos adecuados para concretar, de acuerdo con el artículo 133, y como principio de actuación de la Administración de la Junta de Andalucía, la obligación de servir con objetividad al interés general y actuar de acuerdo, entre otros, con los principios de racionalidad organizativa, simplificación de procedimientos, imparcialidad, transparencia, buena fe, protección de la confianza legítima, no discriminación y proximidad a los ciudadanos, con sujeción a la Constitución, al Estatuto y al resto del ordenamiento jurídico, y por último, desarrollar, en cumplimiento de lo dispuesto en el artículo 134, y como manifestación de la participación ciudadana, el derecho de acceso de los ciudadanos a la Administración de la Junta de Andalucía, que comprenderá en todo caso sus archivos y registros, sin menoscabo de las garantías constitucionales y estatutarias, poniendo a disposición de los mismos los medios tecnológicos necesarios para ello.

La legislación autonómica andaluza cuenta con antecedentes que regulan diversos aspectos de la transparencia. Especial mención merece la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, que en su artículo 3 configura la transparencia como un principio general de organización y funcionamiento, y en el capítulo I del título IV regula los derechos de la ciudadanía ante la actuación administrativa.

Asimismo, la Ley 5/2010, de 11 de junio, de Autonomía Local de Andalucía, configura la transparencia, en su artículo 27, como un principio informador de los servicios locales de interés general, al tiempo que, en su artículo 54, ya contiene obligaciones específicas de publicidad activa.

En materia de información ambiental, los avances obtenidos en materia de transparencia son muchos y palpables, derivados de las obligaciones de los convenios internacionales (Convenio de Aarhus), de directivas comunitarias (Directiva 2003/4/CE del Parlamento Europeo y del Consejo, de 28 de enero de 2003, sobre el acceso del público a la información ambiental) y de la Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente, que regulan específicamente esta materia. En Andalucía se ha plasmado con un desarrollo normativo propio: es el caso de la Ley 7/2007, de 9 de julio, de Gestión Integrada

de la Calidad Ambiental de Andalucía, y el Decreto 347/2011, de 22 de noviembre, por el que se regula la estructura y funcionamiento de la Red de Información Ambiental de Andalucía y el acceso a la información ambiental (Rediam).

Las Cortes Generales han aprobado la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, norma de carácter básico. Al amparo de las competencias que el Estatuto de Autonomía atribuye a nuestra comunidad autónoma en la materia, la presente ley tiene por objeto el desarrollo de la normativa básica estatal, en los términos que sienta el artículo 149.1.18.ª de la Constitución en relación con el artículo 47 del Estatuto de Autonomía, ahondando, en la medida de sus posibilidades, en la ampliación del ámbito de la actividad que se somete a la transparencia.

De esta manera, se da respuesta a la proposición no de ley relativa a las medidas legislativas sobre la transparencia y el acceso a la información pública, aprobada por el Pleno del Parlamento de Andalucía el 27 de febrero de 2013, y en la que se instaba al Consejo de Gobierno a que, a partir de los requerimientos establecidos en el Convenio del Consejo de Europa sobre acceso a los documentos públicos, la futura ley andaluza de transparencia sea el referente en materia de transparencia y acceso a la información pública.

V

Esta ley se estructura en seis títulos, el primero de los cuales se dedica a las disposiciones generales. Entre ellas se comprende el objeto y definiciones, así como el ámbito subjetivo de la Ley, que pretende extenderse en Andalucía a todas las personas y entidades que pueden ser depositarias de la información pública. Para ello se atiende a lo que se establece como básico en la legislación nacional y se adapta y extiende en nuestro caso para todas las administraciones, incluidas las actuaciones administrativas del Parlamento andaluz y sin perjuicio del respeto a su autonomía propia. Del mismo modo, la Ley pretende ser de aplicación a las entidades privadas que se financian con fondos públicos y a aquellas otras que participan en la gestión de los servicios públicos sostenidos con fondos públicos, con la idea de que la ciudadanía mantenga su derecho a la transparencia cuando las actuaciones se financian con fondos públicos.

Asimismo, en este título se regulan aspectos nucleares que afectarán al desarrollo de la transparencia que realicen todas las personas y entidades afectadas, mediante el establecimiento de una serie de principios básicos (entre otros, de transparencia, de libre acceso, de responsabilidad, de no discriminación tecnológica, de veracidad, de utilidad y de facilidad) que constituyen una orientación pro transparencia que vinculará a todas las personas y entidades obligadas por la Ley; de derechos y también obligaciones que configuran la relación de la ciudadanía con las administraciones en esta materia, con una orientación clara que huye de los voluntarismos. De esta forma, en Andalucía se establece con claridad qué puede exigir la ciudadanía en materia de transparencia, qué obligaciones debe cumplir y cuáles van a ser los principios que regirán esta materia con independencia del asunto o materia concreta sobre la que se informe.

En el título segundo se agrupan los artículos referidos a la publicidad activa, conteniéndose junto a unas normas generales una profusa relación de contenidos concretos sobre los que la Ley hace ya un pronunciamiento para que estén disponibles, lo solicite la ciudadanía o no. Se trata sin duda de una extensa relación que abarca elementos sumamente variados que entiende la Ley que son de interés para la ciudadanía.

Cabe añadir que la relación, aunque es extensa, no es exhaustiva. Antes al contrario, se formula de manera que son elementos mínimos y generales. La idea de partida es la de la puesta a disposición de la información pública de forma progresiva de la manera más amplia y sistemática posible, y que esto se haga con la utilización de las tecnologías y plataformas que posibiliten un acceso universal y gratuito.

La Ley es consciente asimismo de la necesidad de asegurar que la información que se obtenga de las distintas personas y entidades sea mínimamente homogénea. De otro modo, pequeñas diferencias pueden dificultar enormemente la comparación que la ciudadanía pretenda hacer de la información que obtiene de las diferentes personas y entidades obligadas. Por ello la redacción de este título ha sido especialmente cuidadosa en el sentido de no introducir elementos de diferenciación en la redacción con respecto a la normativa básica. Esto permitirá que no puedan usarse diferencias de redacción como justificación

para apartarse de los estándares comunes en el suministro de información que manejan todas las administraciones en asuntos similares. Además se introducen novedades importantes y, sobre todo, se establece una clara vocación de ampliación y actualización permanente de la información que se quiere hacer disponible por esta vía.

La regulación jurídica del principio de transparencia en la Administración supone la necesidad de completar dos facetas diferenciadas de la propia transparencia en la actividad de la Administración. Por un lado, todo aquello que supone la información proactiva, es decir, aquella que las propias instituciones públicas ofrecen para el conocimiento de la ciudadanía de modo general, utilizando el mecanismo de las nuevas tecnologías de la información. La segunda faceta de la transparencia es la que se refiere a la entrega por parte de la entidad pública de la información, como contestación a una demanda concreta de alguna persona, sobre cualquier asunto relacionado con la Administración y acerca del cual tenga interés por conocer algún aspecto. A esta se refiere el contenido del título III, bajo la rúbrica de «El derecho de acceso a la información pública».

Quizás pueda ser esta la faceta de la transparencia que sirva para reconocer que con su aplicación efectiva es preciso asumir un cambio de mentalidad profundo que supone para todos aquellos que intervienen en el ámbito de la Administración Pública. La herencia decimonónica basada en la reserva ha justificado una mentalidad hasta ahora opaca y quizás oscurantista y acostumbrada a que su trabajo o resultados no sean accesibles al público y generalmente conocidos.

La Ley reconoce la aplicación subjetiva a toda persona, lo que lleva aparejado que no sólo tendrá legitimación cualquier tipo de persona jurídica para demandar la información, sino también las personas físicas, cualquiera que sea su nacionalidad. Esto supone una importante ampliación en relación con la regulación de otros derechos.

A la obligación legal que se contrae con respecto a la entrega de la información por parte de la propia Administración, formulada de modo tan amplio, es evidente que le son de aplicación las limitaciones que se encuentran establecidas en la normativa básica. En la Ley se contempla como mera remisión en lo que supone de hecho la voluntad de no establecer otros más amplios e, incluso, matizar la invocación que pueda hacerse de algunos de esos límites para negar el acceso.

En ese ámbito de organización que ahora pasará a ser proclive a la transparencia en general, es importante que el procedimiento que se configura para demandar la información sea lo más simple y escueto, sin sujeción a formalidades. Por ello se opta por una remisión a la normativa básica que nuevamente encierra una voluntad de no establecer más requisitos o dificultades de las que sean imprescindibles. Las novedades que se incorporan en estos aspectos van dirigidas a facilitar el ejercicio del derecho de acceso. Para ello se establece el fomento de la tramitación electrónica, la limitación en el uso de las causas de inadmisión, el deber de auxilio y colaboración y otras normas que se establecen desde la óptica de facilitar a la ciudadanía el ejercicio de su derecho.

El título IV se dedica al fomento de la transparencia. Para ello se parte de la obligación de integrar la transparencia en la gestión. La transparencia debe ser transversal e impregnar el actuar de las distintas entidades. De la misma forma se articulan medidas en relación con la conservación de la información y su soporte, que permitirán facilitar la interoperabilidad entre administraciones. Y no pueden olvidarse, en una materia que afecta tanto a las personas profesionales como a la ciudadanía, dos elementos esenciales para transformar la cultura y la práctica de nuestras administraciones, que son la formación y la difusión. Es imprescindible dotar a las personas profesionales que van a atender estas demandas de la necesaria formación y facilitar a la ciudadanía el conocimiento de qué información resulta accesible y cuáles son los cauces disponibles para realizar ese acceso.

Los aspectos organizativos se recogen en el título V, estructurado en dos capítulos.

En el primero de estos capítulos se recogen elementos para la coordinación y planificación de la transparencia en el ámbito de la Junta de Andalucía. Los principios proclamados en el título primero y la voluntad de transparencia que impregna la Ley requieren de instrumentos que en la práctica permitan aplicar la transparencia de forma homogénea y efectiva en el ámbito de cada Administración. Sin perjuicio de las medidas que cada entidad adopte en su propio ámbito, la Administración de la Junta de Andalucía se coordinará a través de la Comisión General de Viceconsejeros y Viceconsejeras. En cada

consejería se establecerá la unidad de transparencia para impulsarla en su ámbito y una comisión de transparencia que garantice la aplicación homogénea. De esta forma existirán planes operativos en cada consejería bajo la planificación directiva y seguimiento del órgano superior de coordinación.

El capítulo segundo crea el Consejo de Transparencia y Protección de Datos de Andalucía como entidad dotada de autonomía e independencia para actuar como autoridad independiente de control tanto en el ámbito de la transparencia como en el de la protección de datos. Se ha configurado como órgano de los previstos en la disposición adicional segunda de la Ley 9/2007, de 22 de octubre, de la Administración Pública, es decir, como una más de aquellas entidades con régimen de independencia funcional o de especial autonomía.

Este órgano estará dotado de independencia orgánica y funcional, y autonomía con respecto a la Administración de la Junta de Andalucía, con respecto al ejercicio de las potestades que se le adscriban, y con personalidad jurídica diferenciada y plena capacidad jurídica y de obrar, patrimonio y tesorería propios, así como autonomía de gestión. Su independencia, por tanto, con respecto a la Administración autonómica es máxima, y su prestigio futuro sólo podrá venir determinado por el rigor de sus actuaciones y resoluciones de control, una vez que empiece a realizar su actividad.

En primer lugar, cabe destacar la unificación bajo la misma entidad de la autoridad independiente en materia de transparencia con la correspondiente a protección de datos. El artículo 82 del Estatuto de Autonomía atribuye a la Comunidad Autónoma la competencia ejecutiva en materia de protección de datos, lo cual requiere de una autoridad independiente en los términos que establece la legislación básica en la materia. La identidad de personas y la coincidencia en muchos aspectos de su trabajo, con el que debe asumir la autoridad independiente en materia de transparencia, así como la evidente interconexión entre ambas materias, hacen aconsejable la unificación bajo una misma autoridad de ambas funciones. Con ello se conseguirá no sólo una economía organizativa, ineludible por otra parte, sino también y sobre todo la coherencia en la aplicación de los criterios que deben regir el actuar de las personas y entidades obligadas por la Ley cuando facilitan información pública a la ciudadanía.

Para asegurar la independencia del órgano, se ha establecido un sistema especial de provisión en el que se asegura la independencia de su titular, al tiempo que se le dota de inamovilidad en el cargo, siguiendo el ejemplo de autoridades similares. Hay en ello un importante paso en el que se someten todas las personas y entidades obligadas por la Ley a un control y supervisión de su actuación por una entidad solvente, independiente y no sujeta a la disponibilidad de ninguna autoridad que no sea la que deriva del principio de legalidad.

Asimismo se crea dentro de esta entidad independiente un órgano de participación, que se ha denominado Comisión Consultiva de la Transparencia y la Protección de Datos, en el que estarán representadas las personas y entidades afectadas por la Ley, expertos y otras entidades que puedan establecerse reglamentariamente. Es un modelo similar al de instituciones análogas que ha demostrado ya en otras administraciones su utilidad práctica.

El título VI regula el régimen sancionador. Se trata de dar respuesta a una cuestión ampliamente demandada por las organizaciones promotoras de la transparencia y por la ciudadanía. Con ello, Andalucía se sitúa en la vanguardia de la transparencia en nuestro país, arbitrando los mecanismos necesarios y adecuados para que la nueva cultura de la transparencia no quede en una mera declaración de intenciones. El decidido compromiso de nuestra comunidad autónoma con la transparencia, la democracia y la ciudadanía se traduce en el establecimiento de este régimen, que persigue no tanto actuar como mecanismo coercitivo o represor, como garantizar y hacer efectivo el derecho de la ciudadanía a la transparencia pública.

La parte final consta de siete disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y cinco disposiciones finales.

La disposición adicional primera tiene por objeto establecer un proceso de revisión y simplificación normativa, lo que ha de redundar en una mejora de la normativa que clarifique la misma de cara a la ciudadanía.

La disposición adicional segunda establece diversas medidas de mejora de la claridad de la regulación previendo el establecimiento de la memoria de análisis de impacto normativo y

la aprobación de unas instrucciones de técnica normativa que doten de homogeneidad a los textos normativos en sus aspectos formales, lo que ha de redundar en la mayor coherencia de nuestro ordenamiento jurídico, amén de servir de guía en la redacción de dichos textos.

La disposición adicional tercera da cumplimiento a lo dispuesto en el artículo 38 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La disposición adicional cuarta se refiere a la supletoriedad de la ley con respecto a las materias que cuentan ya con un régimen jurídico específico de acceso a la información.

La disposición adicional quinta indica las necesarias concordancias de la Ley con la norma estatal, dado el carácter de básico de esta última.

La disposición adicional sexta prevé la creación de la Comisión Consultiva de Subvenciones y Ayudas. Se trata de un órgano de naturaleza consultiva llamado a realizar una importante función preventiva en la materia mediante la doctrina que establezca en sus informes, recomendaciones o instrucciones, coadyuvando al establecimiento de criterios homogéneos. Se trata de una medida complementaria de transparencia, que se manifestará igualmente a través de la publicidad de sus informes, instrucciones y recomendaciones.

La disposición adicional séptima prevé la publicidad en el perfil del contratante de los procedimientos negociados sin publicidad. Se trata de una medida complementaria de transparencia en materia de contratación, que tiene por objeto, sin perjuicio de la simplificación del procedimiento que prevé la normativa básica en estos casos, el facilitar una mayor concurrencia en la adjudicación de este tipo de contratos.

Las disposiciones transitorias primera y segunda regulan el régimen de transición de las solicitudes de acceso a la información presentadas con anterioridad a la entrada en vigor de la Ley y la aplicación de las obligaciones de transparencia a relaciones jurídicas anteriores.

La disposición derogatoria única se refiere a la derogación de preceptos que se opongan al contenido de la propia Ley.

Las disposiciones finales primera a tercera inclusive se refieren a la adecuación de preceptos de otras leyes anteriores que necesitan ser acomodados a lo dispuesto en la presente ley, por lo que se procede a modificar determinados preceptos de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía; de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, y de la Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía.

La disposición final cuarta determina el desarrollo reglamentario de la Ley.

Y por último, la disposición final quinta se refiere a la entrada en vigor de la ley, estableciendo una vacatio legis de un año, tiempo que se estima prudente para preparar a la Administración con respecto a las nuevas obligaciones que se le atribuyen, tanto con respecto a la preparación del personal como con lo que se refiere al tratamiento y difusión de la información. Y se respeta el plazo que la ley básica establece para las entidades locales.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente ley tiene por objeto la regulación, en el ámbito de la Comunidad Autónoma de Andalucía, de la transparencia en su doble vertiente de publicidad activa y de derecho de acceso a la información pública, como instrumento para facilitar el conocimiento por la ciudadanía de la actividad de los poderes públicos y de las entidades con financiación pública, promoviendo el ejercicio responsable de dicha actividad y el desarrollo de una conciencia ciudadana y democrática plena.

Artículo 2. *Definiciones.*

A los efectos de la presente ley, se entiende por:

a) Información pública: los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguna de las personas y entidades incluidas en el presente título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

b) Publicidad activa: la obligación de las personas y entidades a las que hacen referencia los artículos 3 y 5 de hacer pública por propia iniciativa, en los términos previstos en la presente ley, la información pública de relevancia que garantice la transparencia de su actividad relacionada con el funcionamiento y control de su actuación pública.

c) Acceso a la información pública: posibilidad de acceder a la información pública que obre en poder de las entidades sujetas al ámbito de la presente ley con seguridad sobre su veracidad y sin más requisitos que los establecidos en la misma y en la normativa básica estatal.

d) Portal de la Junta de Andalucía: dirección electrónica disponible a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a la Administración de la Junta de Andalucía, que tiene por objeto poner a disposición de la ciudadanía toda clase de servicios e informaciones relacionadas con la Comunidad Autónoma de Andalucía de manera totalmente gratuita, de acuerdo con lo dispuesto en la normativa reguladora de la información y atención a la ciudadanía y la tramitación de procedimientos administrativos por medios electrónicos.

Artículo 3. *Ámbito subjetivo de aplicación.*

1. Las disposiciones de esta ley se aplicarán a:

a) La Administración de la Junta de Andalucía.

b) El Consejo Consultivo de Andalucía, el Consejo Económico y Social de Andalucía y el Consejo Audiovisual de Andalucía.

c) Las agencias de la Administración de la Junta de Andalucía, sean administrativas, de régimen especial o públicas empresariales, así como las entidades de derecho público a las que hace referencia la disposición adicional segunda de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.

d) Las entidades que integran la Administración local andaluza.

e) Los entes instrumentales de derecho público vinculados o dependientes de las administraciones locales andaluzas y, en particular, las agencias públicas administrativas locales, las agencias públicas empresariales locales y las agencias locales de régimen especial.

f) Las universidades públicas andaluzas y sus entidades instrumentales, como pueden ser las sociedades mercantiles de capital mayoritario de las universidades y las fundaciones públicas universitarias.

g) Cualesquiera otras entidades de derecho público con personalidad jurídica vinculadas a las administraciones públicas andaluzas o dependientes de ellas.

h) Las corporaciones de derecho público andaluzas y entidades asimilables, como federaciones y clubes deportivos, en lo relativo a sus actividades sujetas al Derecho administrativo.

i) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50 por ciento. En todo caso, las sociedades mercantiles del sector público andaluz a las que se refiere el artículo 4 del Texto Refundido de la Ley General de la Hacienda Pública de la Junta de Andalucía, aprobado por Decreto Legislativo 1/2010, de 2 de marzo, y las sociedades mercantiles locales y las sociedades interlocales de los artículos 38 y 39 de la Ley 5/2010, de 11 de junio, de Autonomía Local de Andalucía, o normativa que las sustituya.

j) Las fundaciones del sector público previstas en la legislación en materia de fundaciones dependientes de las entidades contempladas en este artículo. En todo caso, las fundaciones del sector público andaluz del artículo 55 de la Ley 10/2005, de 31 de mayo, de Fundaciones de la Comunidad Autónoma de Andalucía, y las fundaciones públicas locales del artículo 40 de la Ley 5/2010, de 11 de junio, de Autonomía Local de Andalucía, o normativa que las sustituya.

k) Las asociaciones constituidas por las administraciones, organismos y entidades previstos en este artículo. Se incluyen los órganos de cooperación previstos en el artículo 5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en la medida en que, por su peculiar naturaleza y por carecer de una estructura administrativa propia, les resulten aplicables las

disposiciones de este título. En estos casos, el cumplimiento de las obligaciones derivadas de la presente ley será llevado a cabo por la Administración que ostente la Secretaría del órgano de cooperación.

l) Las demás entidades con personalidad jurídica propia no incluidas en los apartados anteriores, en las que sea mayoritaria la representación, directa o indirecta, de la Administración de la Junta de Andalucía, a las que hace referencia el artículo 5.1 del Texto Refundido de la Ley General de la Hacienda Pública de la Junta de Andalucía.

m) Los consorcios, fundaciones y demás entidades con personalidad jurídica a los que hace referencia el artículo 5.2 del Texto Refundido de la Ley General de la Hacienda Pública de la Junta de Andalucía.

n) Los fondos a los que hace referencia el artículo 5.3 del Texto Refundido de la Ley General de la Hacienda Pública de la Junta de Andalucía.

2. El Parlamento de Andalucía, el Defensor del Pueblo Andaluz y la Cámara de Cuentas de Andalucía estarán sujetos a la legislación básica del Estado en la materia y a las disposiciones de la presente ley en lo que afecta al ejercicio de sus funciones de carácter administrativo, sin perjuicio de lo que establezca el Parlamento de Andalucía en ejercicio de la autonomía que le garantiza el artículo 102 del Estatuto de Autonomía para Andalucía.

3. A los efectos de lo previsto en los artículos 4.4, 12, 13 y 14 de esta ley, se entienden por administraciones públicas andaluzas los organismos y entidades incluidos en las letras a) a g) del apartado 1.

4. El ámbito previsto en este artículo se entiende sin perjuicio de las obligaciones concretas que establece esta ley para otros órganos o entidades.

Artículo 4. *Obligación de suministrar información.*

1. Las personas físicas y jurídicas distintas de las referidas en el artículo anterior que presten servicios públicos o ejerzan funciones delegadas de control u otro tipo de funciones administrativas estarán obligadas a suministrar a la Administración, organismo o entidad de las previstas en el artículo 3.1 a la que se encuentren vinculadas, previo requerimiento y en un plazo de quince días, toda la información necesaria para el cumplimiento por aquellas de las obligaciones previstas en esta ley, sin perjuicio de los plazos que puedan establecer las entidades locales en ejercicio de su autonomía.

2. Esta obligación se extenderá a las personas adjudicatarias de contratos del sector público en los términos previstos en el respectivo contrato. A estos efectos, los pliegos de cláusulas administrativas particulares o documento contractual equivalente especificarán dicha obligación.

3. Esta obligación será igualmente exigible a las personas beneficiarias de las subvenciones en los términos previstos en las bases reguladoras de las subvenciones y en la resolución de concesión. A estos efectos, las bases reguladoras de la concesión de subvenciones, las resoluciones de concesión o los convenios que instrumenten la concesión de subvenciones recogerán de forma expresa esta obligación.

4. Las administraciones públicas andaluzas podrán acordar, previo apercibimiento y audiencia al interesado, la imposición de multas coercitivas una vez transcurrido el plazo conferido en el requerimiento sin que el mismo hubiera sido atendido. La multa, de 100 a 1.000 euros, será reiterada por períodos de quince días hasta el cumplimiento. El total de la multa no podrá exceder del 5% del importe del contrato, subvención o instrumento administrativo que habilite para el ejercicio de las funciones públicas o la prestación de los servicios. Si en dicho instrumento no figurara una cuantía concreta, la multa no excederá de 3.000 euros. Para la determinación del importe se atenderá a la gravedad del incumplimiento y al principio de proporcionalidad, entre otros.

5. Los medios personales y materiales necesarios para el cumplimiento de las obligaciones establecidas en este artículo serán valorados por las administraciones, organismos o entidades previstas en el artículo 3.1 y, a tal fin, deberán establecerse las previsiones necesarias en los contratos del sector público y en las bases reguladoras de las subvenciones para posibilitar su observancia.

Artículo 5. *Otros sujetos obligados.*

1. Los partidos políticos, organizaciones sindicales y organizaciones empresariales, en todo caso, y las iglesias, confesiones, comunidades y otras entidades inscritas en el Registro de Entidades Religiosas, las corporaciones, asociaciones, instituciones, entidades representativas de intereses colectivos y otras entidades que perciban durante el período de un año ayudas o subvenciones públicas en cuantía superior a 100.000 euros o cuando al menos el 40 por ciento del total de sus ingresos anuales tengan carácter de ayuda o subvención pública, siempre que alcancen como mínimo 5.000 euros, deberán cumplir las obligaciones de transparencia establecidas en la legislación básica.

No obstante, con independencia de los límites anteriores, cuando estas entidades accedan a la financiación de sus actividades y funcionamiento ordinario a través de subvenciones y ayudas financiadas con cargo al presupuesto de la Junta de Andalucía, podrán ser sometidas, además, a exigencias de publicidad específicas aplicando criterios de transparencia análogos a los previstos en materia de publicidad activa en esta ley para las entidades sujetas, en los términos que establezcan las disposiciones de desarrollo de esta ley y las correspondientes convocatorias, respetando en todo caso la naturaleza privada de estas entidades y las finalidades que las mismas tienen reconocidas.

2. Asimismo las normas reguladoras de los conciertos y otras formas de participación de entidades privadas en los sistemas públicos de educación y deportes, sanidad y servicios sociales establecerán aquellas obligaciones de publicidad activa, de entre las que establece la presente ley, que deban cumplir estas entidades para colaborar en la prestación de estos servicios sufragados con fondos públicos. Estas obligaciones se incluirán en los pliegos o documentos contractuales equivalentes que correspondan.

3. Además de lo previsto en el artículo 4, las empresas prestadoras de servicios públicos locales en régimen de gestión indirecta deberán cumplir con las obligaciones de publicidad activa, de entre las previstas en esta ley, que se determinen reglamentariamente para hacer efectivo el principio de transparencia financiera y en la gestión de los servicios locales de interés general previsto en el artículo 27.8 de la Ley 5/2010, de 11 de junio, de Autonomía Local de Andalucía, que tendrán el carácter de comunes y mínimas y podrán ser complementadas con otras por las entidades locales. Las ordenanzas reguladoras de la prestación del servicio público y los pliegos o documentos equivalentes habrán de recoger dichas obligaciones de publicidad activa.

Artículo 6. *Principios básicos.*

Se tendrán en cuenta en la interpretación y aplicación de la presente ley los siguientes principios básicos:

a) Principio de transparencia, en cuya virtud toda la información pública es en principio accesible y sólo puede ser retenida para proteger otros derechos e intereses legítimos de acuerdo con la Ley.

b) Principio de libre acceso a la información pública, en cuya virtud cualquier persona puede solicitar el acceso a la información pública.

c) Principio de responsabilidad, en cuya virtud las entidades sujetas a lo dispuesto en la presente ley son responsables del cumplimiento de sus prescripciones.

d) Principio de no discriminación tecnológica, en cuya virtud las entidades sujetas al ámbito de aplicación de la presente ley habrán de arbitrar los medios necesarios para hacer efectiva la transparencia, con independencia del medio de acceso a la información.

e) Principio de veracidad, en cuya virtud la información pública ha de ser cierta y exacta, asegurando que procede de documentos respecto de los que se ha verificado su autenticidad, fiabilidad, integridad, disponibilidad y cadena de custodia.

f) Principio de utilidad, en cuya virtud la información pública que se suministre, siempre que sea posible, ha de ser adecuada al cumplimiento de los fines para los que se solicite.

g) Principio de gratuidad, en cuya virtud el acceso a la información y las solicitudes de acceso serán gratuitos, sin perjuicio de las exacciones que puedan establecerse por la expedición de copias o soportes o la transposición de la información a un formato diferente al original.

h) Principio de facilidad y comprensión, en cuya virtud la información se facilitará de la forma que resulte más simple e inteligible atendiendo a la naturaleza de la misma y a las necesidades de las personas con circunstancias especiales que les dificulten el ejercicio del derecho.

i) Principio de accesibilidad, por el que se proporcionará información estructurada sobre los documentos y recursos de información con vistas a facilitar la identificación y búsqueda de la información.

j) Principio de interoperabilidad, en cuya virtud la información será publicada conforme al Esquema Nacional de Interoperabilidad.

k) Principio de reutilización, en cuya virtud se fomentará que la información sea publicada en formatos que permitan su reutilización, de acuerdo con la legislación aplicable en materia de reutilización de la información del sector público.

Artículo 7. *Derechos.*

Se reconocen los siguientes derechos:

a) Derecho a la publicidad activa. Consiste en el derecho de cualquier persona a que los poderes públicos publiquen, en cumplimiento de la presente ley, de forma periódica y actualizada, la información veraz cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública.

b) Derecho de acceso a la información pública. Consiste en el derecho de cualquier persona a acceder, en los términos previstos en esta ley, a los contenidos o documentos que obren en poder de cualesquiera de las personas y entidades incluidas en el ámbito de aplicación de la presente ley y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

c) Derecho a obtener una resolución motivada. Consiste en el derecho de la persona solicitante a que sean motivadas las resoluciones que inadmitan a trámite la solicitud de acceso, que denieguen el acceso, que concedan el acceso tanto parcial como a través de una modalidad distinta a la solicitada, así como las que permitan el acceso cuando haya habido oposición de una tercera persona interesada.

d) Derecho al uso de la información obtenida. Consiste en el derecho a utilizar la información obtenida sin necesidad de autorización previa y sin más limitaciones de las que deriven de esta u otras leyes.

Artículo 8. *Obligaciones.*

Las personas que accedan a información pública en aplicación de lo dispuesto en la presente ley estarán sometidas al cumplimiento de las siguientes obligaciones:

a) Ejercer su derecho con respeto a los principios de buena fe e interdicción del abuso de derecho.

b) Realizar el acceso a la información de forma que no se vea afectada la eficacia del funcionamiento de los servicios públicos, concretándose lo más precisamente posible la petición. A estos efectos la Administración colaborará con la persona solicitante en los términos previstos en el artículo 31.

c) Respetar las obligaciones establecidas en la normativa básica para la reutilización de la información obtenida.

d) Cumplir las condiciones y requisitos materiales para el acceso que se hayan señalado en la correspondiente resolución cuando el acceso se realice de forma presencial en un archivo o dependencia pública.

TÍTULO II

La publicidad activa

Artículo 9. *Normas generales.*

1. Las personas y entidades enumeradas en el artículo 3 publicarán de forma periódica, veraz, objetiva y actualizada la información pública cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y el control de la actuación pública por parte de la ciudadanía y de la sociedad en general y favorecer la participación ciudadana en la misma.

En este sentido, adoptarán las medidas oportunas para asegurar la difusión de la información pública y su puesta a disposición de la ciudadanía de la manera más amplia y sistemática posible.

2. Las obligaciones de transparencia contenidas en este título tienen carácter de mínimas y generales y se entienden sin perjuicio de la aplicación de otras disposiciones específicas que prevean un régimen más amplio en materia de publicidad.

3. Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en la normativa básica y, especialmente, el derivado de la protección de datos de carácter personal. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos.

4. La información pública objeto de publicidad activa estará disponible en las sedes electrónicas, portales o páginas web de las personas y entidades incluidas en el ámbito de aplicación de esta ley de una manera segura y comprensible, garantizando especialmente la accesibilidad universal y la no discriminación tecnológica, con objeto de que todas las personas puedan ejercer sus derechos en igualdad de condiciones e incorporando las características necesarias para garantizar la accesibilidad de aquellas personas o colectivos que lo requieran.

Cuando se trate de entidades sin ánimo de lucro que persigan exclusivamente fines de interés social o cultural y cuyo presupuesto sea inferior a 50.000 euros, el cumplimiento de las obligaciones derivadas de esta ley podrá realizarse utilizando los medios electrónicos puestos a su disposición por la Administración Pública de la que provenga la mayor parte de las ayudas o subvenciones públicas percibidas por dichas entidades.

5. Toda la información estará a disposición de las personas con discapacidad en una modalidad accesible, entendiendo por tal aquella que sea suministrada por medios o en formatos adecuados de manera que resulten accesibles y comprensibles, conforme al principio de accesibilidad universal y diseño para todos.

6. En la redacción de la información que tenga la consideración de publicidad activa, se prestará especial atención a lo previsto en la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía, en lo referente a la utilización de lenguaje no sexista ni discriminatorio.

7. Toda la información pública señalada en este título se publicará y actualizará, con carácter general, trimestralmente, salvo que la normativa específica establezca otros plazos atendiendo a las peculiaridades propias de la información de que se trate y sin perjuicio de los plazos que puedan establecer las entidades locales en ejercicio de su autonomía o de la potestad de la Administración de la Junta de Andalucía y de sus entidades instrumentales para publicar toda la información pública que estime conveniente en plazos más breves.

8. La publicidad activa prevista en este título se configurará de forma que permita la participación ciudadana que sea consecuencia de la información facilitada.

Artículo 10. *Información institucional y organizativa.*

1. Las entidades incluidas en el ámbito de aplicación de esta ley publicarán, en lo que les sea aplicable, información relativa a:

a) Las funciones que desarrollan.

b) La normativa que les sea de aplicación y, en particular, los estatutos y normas de organización y funcionamiento de los entes instrumentales.

c) Su estructura organizativa. A estos efectos, incluirán un organigrama actualizado que identifique a las personas responsables de los diferentes órganos y su perfil y trayectoria profesional y la identificación de las personas responsables de las unidades administrativas.

d) Sede física, horarios de atención al público, teléfono y dirección de correo electrónico.

e) Delegaciones de competencias vigentes.

f) Relación de órganos colegiados adscritos y normas por las que se rigen.

g) Las relaciones de puestos de trabajo, catálogos de puestos o documento equivalente referidos a todo tipo de personal, con indicación de sus retribuciones anuales.

h) Las resoluciones de autorización o reconocimiento de compatibilidad que afecten a los empleados públicos.

i) Acuerdos o pactos reguladores de las condiciones de trabajo y convenios colectivos vigentes.

j) La oferta pública de empleo u otro instrumento similar de gestión de la provisión de necesidades de personal.

k) Los procesos de selección del personal.

l) La identificación de las personas que forman parte de los órganos de representación del personal y el número de personas que gozan de dispensa total de asistencia al trabajo.

m) Las agendas institucionales de los gobiernos.

2. La Administración de la Junta de Andalucía publicará, además, la siguiente información:

a) El inventario de entes de la Comunidad Autónoma de Andalucía.

b) El Inventario General de Bienes y Derechos de la Comunidad Autónoma de Andalucía en los términos que se establezcan reglamentariamente.

c) Plan e informe anual de la Inspección General de Servicios de la Junta de Andalucía.

3. Las entidades locales de Andalucía publicarán, además, la información cuya publicidad viene establecida en la Ley 5/2010, de 11 de junio, así como las actas de las sesiones plenarias.

Artículo 11. *Información sobre altos cargos y personas que ejerzan la máxima responsabilidad de las entidades incluidas en el ámbito de aplicación de la Ley.*

Las entidades previstas en el artículo 3 deberán hacer pública la siguiente información:

a) La identificación de los altos cargos incluidos en el ámbito de aplicación de la normativa sobre incompatibilidades de altos cargos de la Administración de la Junta de Andalucía.

b) Las retribuciones de cualquier naturaleza percibidas anualmente por los altos cargos y por las personas que ejerzan la máxima responsabilidad en las entidades incluidas en el ámbito de la aplicación de esta ley.

c) Las indemnizaciones percibidas, en su caso, con ocasión del cese en el cargo.

d) Las declaraciones de actividades, bienes, intereses y retribuciones de altos cargos de la Administración de la Junta de Andalucía, así como las resoluciones de autorización del desarrollo de actividades durante el desempeño del cargo o tras el cese en el mismo.

e) Las declaraciones anuales de bienes y actividades de las personas representantes locales, en los términos previstos en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. Cuando el reglamento no fije los términos en que han de hacerse públicas estas declaraciones, se aplicará lo dispuesto en la normativa de conflictos de intereses en el ámbito de la Administración General del Estado. En todo caso, se omitirán los datos relativos a la localización concreta de los bienes inmuebles y se garantizará la privacidad y seguridad de sus titulares.

Artículo 12. *Información sobre planificación y evaluación.*

1. Las administraciones públicas, las sociedades mercantiles y las fundaciones públicas andaluzas publicarán los planes y programas anuales y plurianuales en los que se fijen objetivos concretos, así como las actividades, medios y tiempo previsto para su consecución. Su grado de cumplimiento y resultados deberán ser objeto de evaluación y publicación periódica junto con los indicadores de medida y valoración. A esos efectos, se considera

evaluación de políticas públicas el proceso sistemático de generación de conocimiento encaminado a la comprensión integral de una intervención pública para alcanzar un juicio valorativo basado en evidencias respecto de su diseño, puesta en práctica, resultados e impactos. Su finalidad es contribuir a la mejora de las intervenciones públicas e impulsar la transparencia y la rendición de cuentas.

2. Los planes y programas a los que se refiere el apartado anterior se publicarán tan pronto sean aprobados y, en todo caso, en el plazo máximo de 20 días, y permanecerán publicados mientras estén vigentes, sin perjuicio de plazos más breves que puedan establecer las entidades locales en ejercicio de su autonomía.

Artículo 13. *Información de relevancia jurídica.*

1. Las administraciones públicas andaluzas, en el ámbito de sus competencias y funciones, publicarán:

a) Las directrices, instrucciones, acuerdos, circulares o respuestas a consultas planteadas por los particulares u otros órganos, en la medida en que supongan una interpretación del Derecho o tengan efectos jurídicos.

b) Los anteproyectos de ley cuando, tras la preceptiva elevación por la Consejería competente, sean conocidos por el Consejo de Gobierno. Asimismo, los anteproyectos de ley y los proyectos de decretos legislativos se publicarán cuando se soliciten los dictámenes, en su caso, al Consejo Económico y Social de Andalucía y al Consejo Consultivo de Andalucía. Y, finalmente, los proyectos de ley tras su aprobación por el Consejo de Gobierno.

c) Los proyectos de reglamentos cuya iniciativa les corresponda se harán públicos en el momento en que, en su caso, se sometan al trámite de audiencia o información pública. Asimismo, se publicarán cuando se solicite, en su caso, el dictamen del Consejo Económico y Social de Andalucía y el dictamen del Consejo Consultivo de Andalucía. La publicación de los proyectos de reglamentos no supondrá, necesariamente, la apertura de un trámite de audiencia pública.

En el ámbito de las entidades locales, una vez efectuada la aprobación inicial de la ordenanza o reglamento local por el Pleno de la Corporación, deberá publicarse el texto de la versión inicial, sin perjuicio de otras exigencias que pudieran establecerse por las entidades locales en ejercicio de su autonomía.

d) La Memoria de Análisis de Impacto Normativo, así como cualquier otro informe que conforme los expedientes de elaboración de los textos normativos con ocasión de la publicidad de estos.

e) Los documentos que, conforme a la legislación sectorial vigente, deban ser sometidos a un período de información pública durante su tramitación.

f) Relación actualizada de las normas que estén en curso, indicando su objeto y estado de tramitación.

2. La Administración de la Junta de Andalucía mantendrá permanentemente actualizada y a disposición de la ciudadanía la normativa vigente de la Comunidad Autónoma.

3. La Administración de la Junta de Andalucía publicará una relación de las competencias y traspasos de funciones y servicios asumidos por la Comunidad Autónoma de Andalucía.

Artículo 14. *Información sobre procedimientos, cartas de servicio y participación ciudadana.*

Las administraciones públicas andaluzas publicarán la información relativa a:

a) El catálogo actualizado de los procedimientos administrativos de su competencia, con indicación de su objeto, trámites y plazos, así como en su caso los formularios que tengan asociados. Se indicará específicamente aquellos procedimientos que admitan, total o parcialmente, tramitación electrónica.

b) Las cartas de servicios elaboradas con la información sobre los servicios públicos que gestiona la Comunidad Autónoma de Andalucía, los informes sobre el grado de cumplimiento y calidad de los servicios públicos, así como la información disponible que permita su valoración.

c) Una relación de los procedimientos en los que sea posible la participación de la ciudadanía mientras se encuentren en trámite.

Artículo 15. *Información sobre contratos, convenios y subvenciones.*

Las entidades incluidas en el ámbito de aplicación de esta ley deberán hacer pública la información relativa a la gestión administrativa que se indica a continuación:

a) Todos los contratos, con indicación del objeto, duración, el importe de licitación y de adjudicación, el procedimiento utilizado para su celebración, los instrumentos a través de los que, en su caso, se ha publicitado, el número de licitadores participantes en el procedimiento y la identidad del adjudicatario, así como las modificaciones y prórrogas del contrato y la indicación de los procedimientos que han quedado desiertos, los supuestos de resolución de contrato o declaración de nulidad, así como los casos de posibles revisiones de precios y cesión de contratos. Igualmente, serán objeto de publicación las decisiones de desistimiento y renuncia de los contratos y las subcontrataciones que se realicen con mención de las personas adjudicatarias.

La publicación de la información relativa a los contratos menores podrá realizarse trimestralmente.

Asimismo, se publicarán datos estadísticos sobre el porcentaje en volumen presupuestario de contratos adjudicados a través de cada uno de los procedimientos previstos en la legislación de contratos del sector público.

b) La relación de los convenios suscritos, con mención de las partes firmantes, su objeto, plazo de duración, modificaciones realizadas, personas obligadas a la realización de las prestaciones y, en su caso, las obligaciones económicas convenidas. Igualmente, se publicarán las encomiendas de gestión que se firmen, con indicación de su objeto, presupuesto, obligaciones económicas y las subcontrataciones que se realicen con mención de las personas adjudicatarias, procedimiento seguido para la adjudicación e importe de la misma.

c) Las subvenciones y ayudas públicas concedidas con indicación de la convocatoria o la resolución de concesión en el caso de subvenciones excepcionales, el programa y crédito presupuestario al que se imputan, su importe, objetivo o finalidad y personas beneficiarias. No obstante, las subvenciones cofinanciadas con fondos agrícolas europeos se regirán, en lo que se refiere a la publicación de la información sobre los beneficiarios, por lo dispuesto en los artículos 111 y 112 del Reglamento (UE) número 1306/2013 del Parlamento y del Consejo, de 17 de diciembre de 2013, sobre la financiación, gestión y seguimiento de la Política Agrícola Común, o norma que la sustituya.

Artículo 16. *Información económica, financiera y presupuestaria.*

Las personas y entidades incluidas en el ámbito de aplicación de esta ley deberán, en su caso, hacer pública, como mínimo, la información con repercusión económica o presupuestaria que se indica a continuación:

a) Los presupuestos, con descripción de las principales partidas presupuestarias e información actualizada y comprensible sobre su estado de ejecución y sobre el cumplimiento de los objetivos de estabilidad presupuestaria y sostenibilidad financiera de las administraciones públicas y la información de las actuaciones de control en los términos que se establezcan reglamentariamente.

b) Las cuentas anuales que deban rendirse y los informes de auditoría de cuentas y de fiscalización por parte de los órganos de control externo que sobre ellas se emitan.

c) La información básica sobre la financiación de la Comunidad Autónoma con indicación de los diferentes instrumentos de financiación.

d) La Deuda Pública de la Administración con indicación de su evolución, del endeudamiento por habitante y del endeudamiento relativo.

e) El gasto público realizado en campañas de publicidad institucional.

Artículo 17. *Ampliación de las obligaciones de publicidad activa.*

1. En aras de una mayor transparencia en la actividad del sector público andaluz, se fomentará la inclusión de cualquier otra información pública que se considere de interés para la ciudadanía. En este sentido, deberá incluirse aquella información cuyo acceso se solicite con mayor frecuencia.

2. Sin perjuicio de lo anterior, la Administración de la Junta de Andalucía publicará, en la medida en que las posibilidades técnicas y jurídicas lo permitan, toda la información que se haya facilitado en el ejercicio del derecho de acceso a la información pública.

3. El Consejo de Gobierno y las entidades locales, en su ámbito competencial y de autonomía, podrán ampliar reglamentariamente las obligaciones de publicación contempladas en el presente título.

Artículo 18. *Acceso a la publicidad activa.*

1. La información pública objeto de publicidad activa, en el ámbito de la Administración de la Junta de Andalucía y sus entidades instrumentales, estará disponible a través del Portal de la Junta de Andalucía.

2. La Administración de la Junta de Andalucía podrá adoptar otras medidas complementarias y de colaboración con el resto de administraciones públicas para el cumplimiento de las obligaciones de transparencia recogidas en este título. Esta colaboración podrá instrumentarse mediante la suscripción de convenios interadministrativos.

Artículo 19. *Reutilización de la información.*

1. Se podrá reutilizar la información a la que se refieren los artículos anteriores dentro de los límites establecidos por la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, y demás normativa vigente en la materia.

2. A estos efectos, la información que tenga la consideración de publicidad activa se ofrecerá, siempre que sea técnicamente posible, en formatos electrónicos que permitan su redistribución, reutilización y aprovechamiento. La información deberá utilizar estándares abiertos en los términos previstos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Artículo 20. *Auxilio institucional.*

Sin perjuicio de lo previsto en el artículo 18.2, aquellos municipios de menor población o con insuficiente capacidad económica y de gestión podrán cumplir las obligaciones de publicidad activa previstas en el presente título acudiendo a la asistencia técnica de la provincia al municipio, prevista en el artículo 12 de la Ley 5/2010, de 11 de junio, o conforme a lo previsto en el artículo 54 de la citada ley, con respecto a la publicación en sede electrónica de la respectiva Diputación Provincial.

Artículo 21. *Publicidad de los plenos de las entidades locales.*

Cuando las entidades locales celebren sesiones plenarias, facilitarán, salvo que concurran causas justificadas de imposibilidad técnica o económica, su acceso a través de Internet, bien transmitiendo la sesión, bien dando acceso al archivo audiovisual grabado una vez celebrada la misma. En todo caso, las personas asistentes podrán realizar la grabación de las sesiones por sus propios medios, respetando el funcionamiento ordinario de la institución.

Artículo 22. *Transparencia del funcionamiento de los gobiernos.*

1. El Consejo de Gobierno de la Junta de Andalucía y los órganos colegiados de gobierno de los ayuntamientos, diputaciones y mancomunidades de municipios, sin perjuicio del secreto o reserva de sus deliberaciones, harán públicos con carácter previo a la celebración de sus reuniones el orden del día previsto y, una vez celebradas, los acuerdos que se hayan aprobado, así como la información contenida en el expediente que se haya sometido a su consideración, en los términos que se establezcan reglamentariamente.

2. A efectos del cumplimiento de lo previsto en el apartado anterior, y para preservar el respeto a los límites aplicables a la publicidad activa establecidos en esta ley, las consejerías proponentes determinarán con ocasión de la remisión del expediente al Consejo de Gobierno la información respecto de la que deba mantenerse alguna reserva, de acuerdo con la normativa aplicable. La Comisión General de Viceconsejeros y Viceconsejeras establecerá los criterios de coordinación que sean convenientes.

Artículo 23. *Control.*

Sin perjuicio del control interno que establezca cada entidad o Administración de acuerdo con sus propias normas organizativas, el Consejo de Transparencia y Protección de Datos de Andalucía podrá efectuar, por iniciativa propia o como consecuencia de denuncia, requerimientos para la subsanación de los incumplimientos que pudieran producirse de las obligaciones establecidas en este título.

TÍTULO III

El derecho de acceso a la información pública

CAPÍTULO I

Normas generales

Artículo 24. *Derecho de acceso a la información pública.*

Todas las personas tienen derecho a acceder a la información pública veraz en los términos previstos en el artículo 105.b) de la Constitución española y su legislación de desarrollo, y el artículo 31 del Estatuto de Autonomía para Andalucía, sin más limitaciones que las contempladas en la Ley.

Artículo 25. *Límites al derecho de acceso a la información pública.*

1. El derecho de acceso a la información pública sólo podrá ser restringido o denegado en los términos previstos en la legislación básica.

2. Las limitaciones al derecho de acceso sólo serán de aplicación durante el período de tiempo determinado por las leyes o en tanto se mantenga la razón que las justifique. Su aplicación será valorada con respecto a la posibilidad de facilitar el acceso parcial.

3. La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso.

4. Las resoluciones que restrinjan o denieguen el derecho de acceso serán objeto de publicidad, previa disociación de los datos de carácter personal que contuvieran. Cuando la mera indicación de la existencia o no de la información supusiera la vulneración de alguno de los límites al acceso, se hará constar esta circunstancia al desestimarse la solicitud.

Artículo 26. *Protección de datos personales.*

De conformidad con lo previsto en la legislación básica de acceso a la información pública, para la resolución de las solicitudes de acceso a la información pública que contengan datos personales de la propia persona solicitante o de terceras personas, se estará a lo dispuesto en la Ley 19/2013, de 9 de diciembre, y en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 27. *Acceso parcial.*

En el caso de que a la información solicitada le resulte de aplicación alguno de los límites a que se refiere el artículo 25 de esta ley, se otorgará, siempre que sea posible, el acceso parcial a la información pública, de conformidad con lo previsto en la Ley básica de acceso a la información pública.

CAPÍTULO II

El ejercicio del derecho de acceso a la información pública

Artículo 28. *Procedimiento de acceso.*

1. El procedimiento para el ejercicio del derecho de acceso se regirá por lo establecido en la legislación básica en materia de transparencia y por lo previsto en esta ley.

2. Será competente para la resolución del procedimiento el órgano o la entidad que lo sea en la materia a la que se refiera la información solicitada.

3. Cuando la persona interesada conozca la ubicación concreta de un documento o información en un archivo determinado, podrá dirigirse al órgano responsable del mismo en los términos previstos en la legislación en materia de archivos.

Artículo 29. *Fomento de la tramitación electrónica.*

1. Las personas o entidades incluidas en el ámbito de aplicación de esta ley promoverán la presentación de las solicitudes por vía telemática, sin perjuicio de lo previsto en el artículo 6.d).

2. En todo caso tendrán disponibles en sus respectivas sedes electrónicas, portales o páginas web, al menos, los modelos normalizados de solicitud.

3. En el ámbito de la Administración de la Junta de Andalucía, la presentación electrónica de las solicitudes de acceso a la información pública se hará en el Portal de la Junta de Andalucía.

Artículo 30. *Reglas especiales relativas a las causas de inadmisión de las solicitudes de acceso.*

En relación a las causas de inadmisión señaladas en la legislación básica, se aplicarán las siguientes reglas:

a) En el supuesto de que se inadmita la solicitud porque la información esté en curso de elaboración o publicación general, la denegación de información deberá especificar el órgano que elabora dicha información y el tiempo previsto para su conclusión y puesta a disposición.

b) Los informes preceptivos no podrán ser considerados como información de carácter auxiliar o de apoyo para justificar la inadmisión de las solicitudes referidas a los mismos.

c) Asimismo, no se estimará como reelaboración que justifique la inadmisión la información que pueda obtenerse mediante un tratamiento informatizado de uso corriente.

Artículo 31. *Deber de auxilio y colaboración.*

1. Las entidades sujetas a esta ley establecerán en sus respectivas plataformas de información y guías de orientación, para facilitar a las personas que deseen ejercer el derecho de acceso, la orientación necesaria para localizar la información que solicitan y los órganos que la posean.

2. El personal al servicio de estas entidades está obligado a ayudar e informar a las personas que lo requieran sobre la forma y el lugar en que pueden presentar sus solicitudes de acceso a la información.

3. En el cumplimiento de los deberes establecidos en los apartados anteriores, se atenderá especialmente a las necesidades de las personas con discapacidad o con otras circunstancias personales que les dificulten el acceso a la información disponible en las administraciones públicas o a los medios electrónicos.

Artículo 32. *Plazo de resolución y notificación.*

Las solicitudes deberán resolverse y notificarse en el menor plazo posible. En todo caso, en el ámbito de la Administración de la Junta de Andalucía y sus entidades instrumentales, el plazo máximo para dictar y notificar la resolución será de 20 días hábiles desde la recepción de la solicitud por el órgano competente para resolver, prorrogables por igual período en el

caso de que el volumen o la complejidad de la información solicitada lo requiera. Dicha ampliación será notificada a la persona solicitante.

Artículo 33. *Reclamaciones frente a las resoluciones.*

1. Frente a toda resolución expresa o presunta en materia de acceso, podrá interponerse reclamación ante el Consejo de Transparencia y la Protección de Datos de Andalucía, con carácter potestativo y previo a su impugnación en vía contencioso-administrativa. Esta reclamación se regirá por lo establecido en la legislación básica en materia de transparencia y por lo previsto en esta ley.

2. Las resoluciones referentes al derecho de acceso a la información pública que sean dictadas por las instituciones y entidades a que se refiere el artículo 3.1.b) y 3.2 sólo serán recurribles ante la jurisdicción contencioso-administrativa.

3. Las resoluciones del Consejo se publicarán, previa disociación de los datos de carácter personal que contuvieran, por medios electrónicos y en los términos que se establezcan reglamentariamente, una vez se hayan notificado a los interesados. La persona titular de la Dirección del Consejo comunicará al Defensor del Pueblo Andaluz las resoluciones que dicte en aplicación de este artículo.

Artículo 34. *Materialización del acceso a la información pública.*

1. La información solicitada se entregará a la persona solicitante en la forma y formato por ella elegidos, salvo que pueda ocasionar la pérdida o deterioro del soporte original, no exista equipo técnico disponible para realizar la copia en ese formato, pueda afectar al derecho de propiedad intelectual o exista una forma o formato más sencilla o económica para el erario público. En todo caso, si la información que se proporcionase en respuesta a una solicitud de acceso a la información pública fuese en formato electrónico, deberá suministrarse en estándar abierto o, en su defecto, deberá ser legible con aplicaciones informáticas que no requieran licencia comercial de uso.

2. Será gratuito el examen de la información solicitada en el sitio en que se encuentre, así como la entrega de información por medios electrónicos.

3. Las entidades y órganos obligados por la Ley elaborarán, publicarán y pondrán a disposición de las personas solicitantes de información pública el listado de las tasas y precios públicos que sean de aplicación a tales solicitudes, conforme a lo previsto en el artículo 6.g), así como los supuestos en los que no proceda pago alguno. En ningún caso, la imposibilidad o incapacidad de hacer frente a las tasas o precios públicos establecidos podrán ser causa para negar el acceso pleno a una información pública solicitada al amparo de la presente ley, en los términos que reglamentariamente se establezcan.

TÍTULO IV

Fomento de la transparencia

Artículo 35. *Integración de la transparencia en la gestión.*

1. Las entidades a las que se refiere el artículo 3.1 de la presente ley establecerán sistemas para integrar la gestión de solicitudes de información de la ciudadanía en el funcionamiento de su organización interna.

2. Asimismo, establecerán medidas para facilitar la transversalidad de la transparencia en la actividad general de la organización.

Artículo 36. *Conservación de la información.*

1. Las entidades a las que se refiere el artículo 3.1 conservarán la información pública que obre en su poder o en el de otras personas o entidades en su nombre, en los términos establecidos en la normativa vigente.

2. Sin perjuicio de lo previsto en el apartado anterior, dicha información se conservará en estándares abiertos que garanticen su longevidad y manteniendo la capacidad de

transformarlos automáticamente a formatos de fácil reproducción y acceso siempre que sea técnicamente posible.

Artículo 37. *Fomento de iniciativas de interoperabilidad.*

La Administración de la Junta de Andalucía fomentará la interoperabilidad de la información entre administraciones públicas, propiciando iniciativas conjuntas de intercambio de información entre las entidades incluidas en el ámbito de aplicación de esta ley.

Artículo 38. *Formación.*

Las administraciones públicas y entidades incluidas en el ámbito de aplicación de la presente ley establecerán los oportunos instrumentos para facilitar la formación y cualificación profesional de las personas empleadas públicas, en especial las que deban atender las funciones de información en el ámbito de la transparencia, tanto en lo que afecte a la publicidad activa como en el caso de quienes deban atender las solicitudes formuladas en ejercicio del derecho de acceso.

Artículo 39. *Divulgación.*

Las administraciones públicas incluidas en el ámbito de aplicación de esta ley contemplarán dentro de sus actuaciones de divulgación y difusión institucional actuaciones específicamente dirigidas a facilitar el conocimiento por la ciudadanía de la información que resulta accesible y de los cauces disponibles para poder acceder a ella, especialmente en referencia a la accesibilidad que en cada caso esté disponible por medios electrónicos.

TÍTULO V

Organización

CAPÍTULO I

Coordinación y planificación en el ámbito de la Junta de Andalucía

Artículo 40. *Coordinación administrativa.*

1. En el ámbito de la Administración de la Junta de Andalucía y sus entidades y organismos adscritos, la coordinación general en materia de transparencia será ejercida por la Comisión General de Viceconsejeros y Viceconsejeras.

2. Dicha Comisión contará con una secretaría que servirá de soporte para la preparación de los trabajos y como oficina administrativa para la relación con las unidades de transparencia y comisiones de transparencia de cada consejería.

3. La Comisión General de Viceconsejeros y Viceconsejeras establecerá la planificación directiva en materia de transparencia, podrá dictar instrucciones y fijar criterios tanto respecto a la implementación de la publicidad activa como en relación al seguimiento de la planificación operativa que se desarrolle en materia de transparencia por cada una de las consejerías para ellas y sus entidades y organismos adscritos.

Artículo 41. *Unidades y comisiones de transparencia.*

1. En cada consejería existirá una unidad de transparencia cuyas funciones se asignarán a una unidad con nivel orgánico mínimo de servicio, que, a estos efectos, actuará bajo la dependencia de la Viceconsejería con el fin de impulsar la transparencia en el ámbito de la Consejería y sus entidades y organismos adscritos y facilitar la aplicación en ese ámbito de los criterios e instrucciones que se establezcan.

2. Asimismo, se constituirá en cada consejería una comisión de transparencia con la participación de los distintos centros directivos, archivos, entidades instrumentales y demás entidades dependientes para asegurar la implementación de la transparencia de forma homogénea en todos los ámbitos de la actuación administrativa de la Junta de Andalucía.

3. Por Decreto del Consejo de Gobierno se regulará el funcionamiento de las unidades y las comisiones de transparencia.

4. La Inspección General de Servicios de la Junta de Andalucía velará por el cumplimiento de las obligaciones establecidas en los títulos II y III de la presente ley en todo aquello que sea aplicable a la Administración de la Junta de Andalucía y sus entidades instrumentales.

Artículo 42. *Planificación.*

1. En materia de transparencia, cada consejería establecerá un plan operativo que deberá incluir la estructura organizativa, las responsabilidades, las funciones y los procedimientos para realizar la acción de transparencia en el ámbito de la Consejería y sus entidades y organismos adscritos.

2. Estos planes se aprobarán mediante Orden y serán elaborados con la participación de la correspondiente Comisión de Transparencia con arreglo a los criterios y requisitos que se hayan establecido reglamentariamente.

3. Las actuaciones realizadas y su valoración formarán parte de la información pública objeto de publicidad activa.

CAPÍTULO II

Consejo de Transparencia y Protección de Datos de Andalucía

Artículo 43. *Creación y naturaleza.*

1. Se crea el Consejo de Transparencia y Protección de Datos de Andalucía, en adelante el Consejo, como autoridad independiente de control en materia de protección de datos y de transparencia en la Comunidad Autónoma de Andalucía.

2. El Consejo se configura como una entidad pública con personalidad jurídica propia, con plena capacidad y autonomía orgánica y funcional para el ejercicio de sus cometidos.

3. El Consejo ejercerá sus funciones con objetividad, profesionalidad, sometimiento al ordenamiento jurídico y plena independencia de las administraciones públicas en el ejercicio de las mismas.

4. Su relación con la Administración de la Junta de Andalucía se llevará a cabo a través de la Consejería de la Presidencia.

Artículo 44. *Régimen jurídico.*

1. El Consejo tendrá la consideración de Administración institucional a los efectos previstos en la disposición adicional segunda de la Ley 9/2007, de 22 de octubre.

2. El Consejo se regirá por lo dispuesto en esta ley, por lo establecido en la disposición adicional segunda de la Ley 9/2007, de 22 de octubre, y, supletoriamente, por lo dispuesto en la misma ley para las agencias administrativas, así como por lo que dispongan sus estatutos en materia organizativa y de funcionamiento.

3. El régimen presupuestario, patrimonial, económico-financiero, de contabilidad e intervención del Consejo será el establecido en el Texto Refundido de la Ley General de la Hacienda Pública de la Junta de Andalucía y en las demás disposiciones que le sean de aplicación. El régimen de contratación será el establecido para las administraciones públicas en el texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre.

Artículo 45. *Finalidad.*

El Consejo actuará en el territorio de Andalucía como autoridad pública independiente de control en materia de protección de datos en los términos previstos en el artículo 41 de la Ley Orgánica 15/1999, de 13 de diciembre, y como órgano independiente e imparcial garante del derecho a la transparencia, conforme a lo previsto en esta ley y en la legislación básica en la materia.

Artículo 46. *Estructura del Consejo.*

1. El Consejo de Transparencia y Protección de Datos de Andalucía está compuesto por los siguientes órganos:

a) La Comisión Consultiva, con la composición y funciones previstas en el artículo 49.
b) La Dirección, cuyo titular presidirá también la Comisión Consultiva.

2. La constitución efectiva del Consejo tendrá lugar conforme a lo que determinen sus estatutos, que serán aprobados por el Consejo de Gobierno y que contendrán en todo caso su estructura, competencias, organización y funcionamiento.

Artículo 47. *Dirección del Consejo.*

1. La persona que ejerza la Dirección del Consejo será nombrada por el Consejo de Gobierno por un periodo de 5 años no renovable. No obstante, expirado el plazo del mandato correspondiente, continuará en ejercicio de sus funciones hasta la toma de posesión del nuevo titular.
2. La designación corresponde al Parlamento de Andalucía, por mayoría absoluta, y deberá recaer en una persona de reconocido prestigio y competencia profesional.
3. Ejercerá sus funciones con plena independencia y objetividad, y no estará sujeta a instrucción alguna en el desempeño de aquellas. No obstante, la persona que ejerza la Dirección deberá oír a la Comisión Consultiva en aquellas propuestas que esta le realice en el ejercicio de sus funciones.
4. La persona que ejerza la Dirección del Consejo sólo cesará antes de la expiración de su período de mandato por alguna de las siguientes causas:

a) Muerte o incapacitación judicial.
b) Renuncia.
c) Por separación, acordada por el Consejo de Gobierno, previa instrucción de expediente, en el que necesariamente será oída la Comisión Consultiva, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

Artículo 48. *Funciones de la Dirección.*

1. La Dirección del Consejo ejercerá las siguientes funciones:

a) Representar al Consejo.
b) La resolución de las reclamaciones contra las resoluciones expresas o presuntas en materia de acceso que puedan presentarse por las personas solicitantes o por las terceras personas interesadas en los supuestos previstos en la legislación básica.
c) Adoptar criterios de interpretación uniforme de las obligaciones contenidas en esta ley.
d) Presentar ante el Parlamento de Andalucía un informe anual de actuación.
e) Resolver las consultas que en materia de transparencia o protección de datos le planteen las administraciones y entidades sujetas a esta ley.
f) Responder a las consultas que, con carácter facultativo, le planteen los órganos encargados de tramitar y resolver las solicitudes de acceso a la información, así como las consultas que para el cumplimiento de lo previsto en el artículo 22 le planteen los órganos competentes.
g) Ejercer el control de la publicidad activa en los términos previstos en el artículo 23.
h) Instar la incoación de expedientes disciplinarios o sancionadores de acuerdo con las previsiones del título VI.
i) Desempeñar las funciones previstas en la legislación sobre protección de datos para su ejercicio por las agencias autonómicas en su caso.

2. La Dirección del Consejo estará asesorada por la Comisión Consultiva prevista en el artículo 49.

Artículo 49. *Comisión Consultiva de la Transparencia y la Protección de Datos.*

1. La Comisión Consultiva de la Transparencia y la Protección de Datos, en adelante la Comisión, se constituye como órgano de participación y consulta en materia de transparencia y protección de datos.

2. Sus funciones, funcionamiento y composición se determinarán en los estatutos del Consejo.

3. La Comisión Consultiva estará compuesta por la persona que ejerza la Dirección del Consejo y catorce miembros en representación de:

a) La Administración de la Junta de Andalucía.
b) El Parlamento de Andalucía, reuniendo la condición de diputado o diputada.
c) Las administraciones locales andaluzas.
d) Las universidades públicas andaluzas.
e) Las entidades representativas de las personas consumidoras y usuarias.
f) Las entidades representativas de los intereses económicos y sociales.
g) Personas expertas en la materia.
h) Un representante de la Oficina del Defensor del Pueblo Andaluz.
i) Un representante de la Cámara de Cuentas de Andalucía.

4. Los miembros de la Comisión serán nombrados por la persona titular de la Consejería a la que se refiere el artículo 43.4. Serán cesados por las mismas causas que la persona que ejerza la Dirección del Consejo o a petición de la entidad que los hubiera propuesto.

TÍTULO VI

Régimen sancionador

Artículo 50. *Régimen jurídico.*

1. El incumplimiento de las obligaciones establecidas en la presente ley se sancionará conforme a lo previsto en este título, sin perjuicio de otras responsabilidades que pudieran concurrir.

2. La potestad sancionadora respecto de las infracciones tipificadas en esta ley se ejercerá de conformidad con lo dispuesto en ella y en la normativa en materia de régimen jurídico de las administraciones públicas y del procedimiento administrativo sancionador. Las infracciones disciplinarias se regirán por el procedimiento previsto para el personal funcionario, estatutario o laboral que resulte de aplicación en cada caso.

Artículo 51. *Responsables.*

1. Son responsables de las infracciones, aun a título de simple inobservancia, las personas físicas o jurídicas, cualquiera que sea su naturaleza, que realicen acciones o que incurran en las omisiones tipificadas en la presente ley con dolo, culpa o negligencia.

2. En particular, son responsables:

a) Las autoridades, directivos y el personal al servicio de las entidades previstas en el artículo 3.
b) Las personas físicas y jurídicas a las que se refiere el artículo 4.
c) Las entidades a las que se refiere el artículo 5.

Artículo 52. *Infracciones de carácter disciplinario.*

Son infracciones imputables a las autoridades, directivos y el personal al servicio de las entidades previstas en el artículo 3:

1. Infracciones muy graves:

a) El incumplimiento de las obligaciones de publicidad activa previstas en el título II cuando se haya desatendido el requerimiento expreso del Consejo de Transparencia y Protección de Datos de Andalucía.
b) La denegación arbitraria del derecho de acceso a la información pública.

c) El incumplimiento de las resoluciones dictadas en materia de acceso por el Consejo de Transparencia y Protección de Datos de Andalucía en las reclamaciones que se le hayan presentado.

2. Infracciones graves:

a) El incumplimiento reiterado de las obligaciones de publicidad activa previstas en el título II.
b) El incumplimiento reiterado de la obligación de resolver en plazo la solicitud de acceso a la información pública.
c) La falta de colaboración en la tramitación de las reclamaciones que se presenten ante el Consejo de Transparencia y Protección de Datos de Andalucía.
d) Suministrar la información incumpliendo las exigencias derivadas del principio de veracidad, de acuerdo con lo establecido en el artículo 6.e).

3. Infracciones leves:

a) El incumplimiento de las obligaciones de publicidad activa previstas en el título II.
b) El incumplimiento injustificado de la obligación de resolver en plazo la solicitud de acceso a la información pública.

Artículo 53. *Infracciones de las personas obligadas al suministro de información.*

Son infracciones imputables a las personas físicas y jurídicas a las que se refiere el artículo 4:

1. Muy graves:

a) El incumplimiento de la obligación de suministro de información que haya sido reclamada como consecuencia de un requerimiento del Consejo de Transparencia y Protección de Datos de Andalucía o para dar cumplimiento a una resolución del mismo en materia de acceso.
b) La reincidencia en la comisión de faltas graves. Se entenderá por reincidencia la comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme.

2. Graves:

a) La falta de contestación al requerimiento de información.
b) Suministrar la información incumpliendo las exigencias derivadas del principio de veracidad, de acuerdo con lo establecido en el artículo 6.e).
c) La reincidencia en la comisión de faltas leves. Se entenderá por reincidencia la comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme.

3. Leves:

a) El retraso injustificado en el suministro de la información.
b) El suministro parcial o en condiciones distintas de las reclamadas.

Artículo 54. *Infracciones de otras entidades.*

Son infracciones imputables a las entidades de naturaleza privada a las que se refiere el artículo 5:

1. Infracción muy grave: el incumplimiento de las obligaciones de publicidad activa que les sean de aplicación cuando se haya desatendido el requerimiento expreso del Consejo de Transparencia y Protección de Datos de Andalucía.
2. Infracción grave: el incumplimiento reiterado de las obligaciones de publicidad activa que les sean de aplicación o publicar la información incumpliendo las exigencias derivadas del principio de veracidad.
3. Infracción leve: el incumplimiento de las obligaciones de publicidad activa que sean de aplicación cuando no constituya infracción grave o muy grave.

Artículo 55. *Sanciones disciplinarias.*

1. A las infracciones del artículo 52, imputables a personal al servicio de las entidades previstas en el artículo 3, se les aplicarán las sanciones que correspondan con arreglo al régimen disciplinario que en cada caso resulte aplicable.

2. Cuando las infracciones sean imputables a autoridades y directivos, podrán aplicarse las siguientes sanciones:

a) Amonestación en el caso de infracciones leves.

b) En el caso de infracciones graves:

1.º Declaración del incumplimiento y publicación en el boletín oficial correspondiente.

2.º Cese en el cargo.

c) En el caso de muy graves:

1.º Todas las previstas para infracciones graves.

2.º No poder ser nombrados para ocupar cargos similares por un período de hasta tres años.

Artículo 56. *Sanciones a otras entidades.*

1. Para las infracciones previstas en los artículos 53 y 54, podrán aplicarse las sanciones de amonestación y multa.

2. Las infracciones leves podrán sancionarse con amonestación o multa comprendida entre 200 y 5.000 euros.

3. Las infracciones graves se sancionarán con multa comprendida entre 5.001 y 30.000 euros.

4. Las infracciones muy graves se sancionarán con multa comprendida entre 30.001 y 400.000 euros.

5. Las infracciones graves y muy graves podrán conllevar como sanción accesoria el reintegro total o parcial de la subvención concedida o, en su caso, la resolución del contrato, concierto o vínculo establecido. Para la imposición y graduación de estas sanciones accesorias, se atenderá a la gravedad de los hechos y su repercusión, de acuerdo con el principio de proporcionalidad.

Artículo 57. *Procedimiento.*

1. Para la imposición de las sanciones establecidas en el presente título, se seguirán las disposiciones previstas en el procedimiento sancionador o, en el caso de infracciones imputables al personal al servicio de entidades, el régimen disciplinario funcionarial, estatutario o laboral que en cada caso resulte aplicable.

2. En todo caso, el procedimiento se iniciará de oficio, por acuerdo del órgano competente, bien por propia iniciativa o como consecuencia de orden superior, petición razonada de otros órganos o denuncia de la ciudadanía. El Consejo de Transparencia y Protección de Datos de Andalucía, cuando constate incumplimientos en esta materia susceptibles de ser calificados como alguna de las infracciones previstas en este título, instará la incoación del procedimiento. En este último caso, el órgano competente estará obligado a incoar el procedimiento y a comunicar al Consejo el resultado del mismo.

Artículo 58. *Competencia sancionadora.*

1. La competencia para la imposición de sanciones disciplinarias corresponderá al órgano que determine la normativa aplicable en la Administración o entidad a la que pertenezca el sujeto infractor.

2. Para las infracciones previstas en el artículo 53, la competencia corresponderá al órgano que determine la normativa aplicable en la Administración o entidad a la que se encuentre vinculada la persona infractora.

3. En el supuesto de infracciones de las tipificadas en el artículo 54, la potestad sancionadora será ejercida por la Consejería de la Junta de Andalucía competente en materia de la presidencia o por la entidad local titular del servicio público.

Disposición adicional primera. *Revisión y simplificación normativa.*

1. Todas las administraciones públicas andaluzas habrán de acometer una revisión, simplificación y, en su caso, una consolidación normativa de sus ordenamientos jurídicos. Para ello, habrán de efectuar los correspondientes estudios, derogar las normas que hayan quedado obsoletas y determinar, en su caso, la necesidad de introducir modificaciones, novedades o proponer la elaboración de un texto refundido, de conformidad con las previsiones constitucionales y legales sobre competencia y procedimiento a seguir, según el rango de las normas que queden afectadas.

2. A tal fin, en el ámbito de la Administración de la Junta de Andalucía, la Consejería competente en materia de administración pública elaborará un plan de calidad y simplificación normativa y se encargará de coordinar el proceso de revisión y simplificación normativa respecto del resto de las consejerías.

3. Las secretarías generales técnicas de las distintas consejerías llevarán a cabo el proceso de revisión y simplificación en sus ámbitos competenciales de actuación.

Disposición adicional segunda. *Mejora de la calidad de regulación.*

En el marco de lo dispuesto en el capítulo I del título I de la Ley 2/2011, de 4 de marzo, de Economía Sostenible, se realizarán las siguientes actuaciones:

a) Mediante Decreto del Consejo de Gobierno se regulará, como trámite preceptivo en los procedimientos de aprobación de los anteproyectos de ley, decretos legislativos y disposiciones de carácter general, una memoria de análisis de impacto normativo.

b) Por Acuerdo del Consejo de Gobierno, se aprobarán unas instrucciones de técnica normativa al objeto de homogeneizar los aspectos formales de los textos normativos de la Comunidad Autónoma.

Disposición adicional tercera. *Designación de representante de la Comunidad Autónoma de Andalucía en la Agencia Española de Protección de Datos.*

A efectos de lo dispuesto en el artículo 38 de la Ley Orgánica 15/1999, de 13 de diciembre, el director o directora del Consejo de Transparencia y Protección de Datos de Andalucía ostentará la condición de representante de la Comunidad Autónoma en el Consejo Consultivo de la Agencia Española de Protección de Datos.

Disposición adicional cuarta. *Regulaciones especiales del derecho de acceso a la información pública.*

1. La normativa reguladora del correspondiente procedimiento administrativo será la aplicable al acceso por parte de quienes tengan la condición de interesados en un procedimiento administrativo en curso a los documentos que se integren en el mismo.

2. Se regirán por su normativa específica, y por esta ley con carácter supletorio, aquellas materias que tengan previsto un régimen jurídico específico de acceso a la información.

3. En este sentido, esta ley será de aplicación, en lo no previsto en sus respectivas normas reguladoras, al acceso a la información ambiental y a la destinada a la reutilización.

Disposición adicional quinta. *Conformidad con la normativa estatal.*

El contenido de la letra a) del artículo 2; las letras e), g), h), i), j) y k) del apartado 1, así como los apartados 2 y 3 del artículo 3; los apartados 1 y 2 del artículo 4; el párrafo primero del apartado 1 del artículo 5; las letras i), j) y k) del artículo 6; el primer párrafo del apartado 1 y los apartados 2, 3 y 5 del artículo 9; las letras a), b), c) y h) del apartado 1 del artículo 10; las letras b), c) y e) del artículo 11; el apartado 1 del artículo 12; las letras a), b), c), d) y e) del artículo 13.1; el artículo 15; las letras a) y b) del artículo 16; el apartado 2 del artículo 18; el artículo 24; los apartados 3 y 4 del artículo 25; el artículo 33, y el apartado 2 del artículo 34 de la presente ley están redactados, total o parcialmente, de conformidad con los preceptos de aplicación general de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

Disposición adicional sexta. *Comisión Consultiva de Subvenciones y Ayudas.*

1. Se creará, por Decreto del Consejo de Gobierno, la Comisión Consultiva de Subvenciones y Ayudas como órgano colegiado consultivo en materia de subvenciones y ayudas, de los órganos y entidades que integran el sector público autonómico, así como de las entidades locales andaluzas.
2. La norma de creación regulará su composición, funcionamiento y competencias.
3. Los informes, recomendaciones o instrucciones que emita serán públicos.

Disposición adicional séptima. *Transparencia en los procedimientos negociados sin publicidad.*

La información relativa a los contratos a que se refiere el artículo 168 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, se deberá publicar de forma diferenciada en un apartado de la Sección de Transparencia del Portal de la Junta de Andalucía a fin de facilitar su identificación y búsqueda de acuerdo con el principio de accesibilidad del artículo 6.i) de la presente Ley.

Disposición transitoria primera. *Solicitudes de acceso en trámite.*

Las solicitudes de acceso a información pública presentadas con anterioridad a la entrada en vigor de la presente ley continuarán su tramitación con arreglo a la normativa aplicable en el momento de su presentación.

Disposición transitoria segunda. *Aplicación de obligaciones de transparencia a relaciones jurídicas anteriores.*

Las obligaciones establecidas en los artículos 4 y 5 nacen de la Ley y, en consecuencia, no será obstáculo para su exigibilidad, a partir de la entrada en vigor de esta ley, el mero hecho de que el contrato, subvención o cualesquiera otras formas de relación, estando vigentes, tengan su origen en una fecha anterior.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente ley.

Disposición final primera. *Modificación de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía.*

El artículo 31 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, queda redactado como sigue:

> **«Artículo 31.** *Transparencia.*
>
> 1. El Gobierno actuará en su funcionamiento con transparencia y hará público con carácter previo a la celebración de sus reuniones el orden del día previsto y, una vez celebradas, los acuerdos que se hayan aprobado.
> 2. En todo caso, las deliberaciones del Consejo de Gobierno, así como las opiniones o votos emitidos en él, tendrán carácter secreto, estando obligados sus integrantes a mantener dicho carácter, aun cuando hubieran dejado de pertenecer al Consejo de Gobierno.
> 3. La información contenida en los expedientes de los asuntos sometidos al Consejo de Gobierno estará sujeta a los criterios y reglas generales de acceso establecidos en la legislación en materia de transparencia, aplicándose estos por las consejerías que los hayan tramitado.»

Disposición final segunda. *Modificación de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.*

Se modifica la Ley 9/2007, de 22 de octubre, de Administración de la Junta de Andalucía, en los siguientes términos:

Uno. El artículo 79 queda redactado del siguiente modo:

«Artículo 79. *Publicidad y transparencia de la actuación administrativa.*

La actuación de la Administración de la Junta de Andalucía se desarrollará con el máximo respeto a los principios de publicidad y transparencia, sin perjuicio de las limitaciones derivadas del derecho a la intimidad o de otros derechos constitucionales que gozan de una protección específica.

Para hacer efectivo estos principios, se reconoce el derecho a la publicidad activa y el derecho de acceso a la información pública en los términos previstos en la Ley de Transparencia Pública de Andalucía.»

Dos. El párrafo primero del apartado 2 del artículo 80 queda redactado del siguiente modo:

«En orden a facilitar el derecho a la información de la ciudadanía, y sin perjuicio de lo dispuesto en la Ley de Transparencia Pública de Andalucía, la Administración de la Junta de Andalucía está obligada: […].»

Tres. El artículo 86 queda redactado del siguiente modo:

«Artículo 86. *Derecho de acceso a la información pública.*

La ciudadanía tiene derecho a acceder a la información pública, archivos y registros en los términos y con las condiciones establecidas en la Constitución, en la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, en la Ley de Transparencia Pública de Andalucía y demás que resulten de aplicación.»

Disposición final tercera. *Modificación de la Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía.*

Se modifica la Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía, en los siguientes términos:

Uno. El artículo 31 queda redactado del siguiente modo:

«Artículo 31. *Comisión Andaluza de Valoración de Documentos.*

1. En el marco de las normas recogidas en la Constitución, en la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, en la Ley de Transparencia Pública de Andalucía, en la presente ley y demás normas que resulten de aplicación, la Comisión Andaluza de Valoración de Documentos es un órgano colegiado de carácter técnico y de participación, al que corresponde la valoración de los documentos de titularidad pública y la aplicación del régimen de acceso material al patrimonio documental de Andalucía custodiado en los archivos del Sistema.

2. La adscripción, composición y funcionamiento de la Comisión Andaluza de Valoración de Documentos se establecerán reglamentariamente.

3. Son funciones de la Comisión Andaluza de Valoración de Documentos:

a) Dictaminar la conservación de aquellos documentos que tengan interés para la Comunidad Autónoma y autorizar la eliminación de aquellos otros que, extinguido su valor probatorio de derechos y obligaciones, carezcan de ese interés, de acuerdo con el procedimiento que reglamentariamente se establezca.

b) Establecer los criterios sobre el acceso material a los documentos de titularidad pública y a los documentos del Patrimonio Documental de Andalucía custodiados en los archivos del Sistema.

c) Establecer los plazos de permanencia, custodia y control de los documentos en los diferentes archivos.

d) Evacuar el informe que declare la conservación de los documentos judiciales en razón de su valor histórico-cultural a que se refiere el artículo 48.2.

e) Evacuar los informes que les sean solicitados por la persona titular de la consejería y por quienes sean titulares de sus direcciones generales en materia de su competencia.

f) Elevar propuestas sobre cualquier otra medida que permita el cumplimiento de sus funciones.

g) Cualesquiera otras funciones que se determinen reglamentariamente.»

Dos. El artículo 61 queda redactado del siguiente modo:

«Artículo 61. *Acceso a los documentos de titularidad pública y a su información.*

El acceso a los documentos de titularidad pública y a su información se ajustará a lo dispuesto en la Constitución, en la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, en la Ley de Transparencia Pública de Andalucía, en la presente ley y demás normas que resulten de aplicación.»

Tres. El artículo 62 queda redactado del siguiente modo:

«Artículo 62. *Derecho de acceso a los documentos de titularidad pública.*

1. El derecho de acceso sólo podrá ser restringido o denegado en aplicación de los límites y causas de inadmisión establecidos en la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, y en la Ley de Transparencia Pública de Andalucía.

2. El acceso material a los documentos podrá ser denegado cuando el estado de conservación de los mismos así lo requiera, pudiendo ser sustituido por una reproducción veraz.

3. Se denegará la consulta directa de los documentos originales a las personas que hayan sido condenadas por sentencia firme por la comisión de delitos contra la seguridad y conservación del Patrimonio Documental. Queda exceptuada de esta limitación la consulta de los documentos pertenecientes a procedimientos en los que sean parte interesada.

4. La Comisión Andaluza de Valoración de Documentos podrá establecer criterios homogéneos sobre la aplicación de la normativa sobre la materialización del acceso a los archivos, en los términos previstos en la legislación sobre transparencia, considerando el estado de conservación de los documentos.»

Cuatro. El apartado 1 del artículo 63 queda redactado del siguiente modo:

«1. El ejercicio del derecho de acceso a los documentos de titularidad pública y obtención de copias de los mismos está sujeto a lo dispuesto en los artículos 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y 86 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, y al procedimiento que se regula en la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, y en la Ley de Transparencia Pública de Andalucía.»

Cinco. El párrafo c) del artículo 72 queda redactado del siguiente modo:

«c) Impedir el derecho de acceso de la ciudadanía a los archivos, contraviniendo los términos previstos en el artículo 65.»

Disposición final cuarta. *Desarrollo reglamentario.*

El desarrollo reglamentario de esta ley se llevará a efecto de acuerdo con lo dispuesto en los artículos 112 y 119.3 del Estatuto de Autonomía para Andalucía y 44 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía.

Disposición final quinta. *Entrada en vigor.*

1. La presente ley entrará en vigor al año de su publicación en el Boletín Oficial de la Junta de Andalucía, salvo lo dispuesto en su título V, que entrará en vigor el 1 de enero de 2015.

2. Las entidades locales andaluzas dispondrán de un plazo máximo de dos años, desde la entrada en vigor de la Ley 19/2013, de 9 de diciembre, para adaptarse a las obligaciones contenidas en esta ley.

§ 30

Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos

Comunidad Autónoma del País Vasco
«BOPV» núm. 3, de 4 de enero de 2024
«BOE» núm. 16, de 18 de enero de 2024
Última modificación: sin modificaciones
Referencia: BOE-A-2024-900

Se hace saber a todos los ciudadanos y ciudadanas de Euskadi que el Parlamento Vasco ha aprobado la Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos.

EXPOSICIÓN DE MOTIVOS

I

El marco normativo en materia de protección de datos personales ha sufrido una importante modificación como consecuencia de la aprobación y plena aplicación, desde el 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Comúnmente se denomina Reglamento General de Protección de Datos.

El Reglamento (UE) 2016/679 es una norma dotada de efecto directo pleno en los estados miembros, e introduce novedades fundamentales, tanto en la regulación sustantiva del derecho fundamental a la protección de datos, como en lo que afecta a la supervisión de dicho derecho por las denominadas autoridades de control, autoridades públicas independientes que cada Estado miembro establecerá con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento, y de facilitar la libre circulación de datos personales en la Unión. Desde la aprobación de las primeras normas reguladoras de la protección de datos personales en el Estado, su régimen de supervisión se ha materializado en la coexistencia de diversas autoridades de control, estatal y autonómicas, con ámbitos competenciales diferenciados.

A su vez, el Reglamento General de Protección de Datos establece un amplio elenco de funciones y potestades a desarrollar por las autoridades de control, que deberán estar dotadas de medios que garanticen adecuadamente su independencia, constituida como un principio esencial de garantía de la adecuada protección del derecho fundamental.

Con la finalidad de adaptar el derecho interno al reglamento, se aprobó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que dedica el capítulo II de su título VII a las denominadas autoridades autonómicas de protección de datos.

Más recientemente, y en transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, se aprobó la Ley Orgánica 7/2021 de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Esta ley orgánica tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección y prevención frente a las amenazas contra la seguridad pública.

Teniendo en cuenta las consideraciones anteriores, se ha elaborado esta ley de protección de datos personales, que tiene por objeto adaptar la organización y funcionamiento de la normativa aplicable en la Comunidad Autónoma del País Vasco a las previsiones del Reglamento (UE) 2016/679; de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; así como de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Así pues, esta ley reemplaza el régimen contenido en la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, y en sus normas de desarrollo, en particular el Decreto 308/2005, de 18 de octubre, por el que se desarrolla la citada Ley 2/2004, y el Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos.

En la elaboración de la ley se ha considerado que el régimen de los principios, derechos y obligaciones que configura el derecho fundamental a la protección de datos personales se encuentra suficientemente regulado con las disposiciones contenidas en el Reglamento General de Protección de Datos, completadas con las previstas en la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, lo que hace innecesario adoptar adicionalmente ninguna disposición relacionada con el contenido sustantivo del derecho fundamental. En el mismo sentido, se ha considerado que ambas normas ya establecen un marco suficientemente claro de obligaciones que no precisa de ser completado por la norma autonómica, so pena de establecer un régimen especialmente burocrático de obligaciones para las administraciones y entidades sometidas a su ámbito de aplicación.

Teniendo en cuenta esta premisa, la ley se ha estructurado en torno a cuatro capítulos, siendo el primero únicamente expresivo de la delimitación del objeto y ámbito de aplicación de la ley. Los tres restantes capítulos regulan el régimen de la Autoridad Vasca de Protección de Datos, que reemplaza a la actual Agencia Vasca de Protección de Datos; el régimen sancionador al que se someten los responsables y encargados del tratamiento comprendidos en el ámbito de aplicación de la ley, y, por último, el procedimiento que se seguirá en los supuestos en los que la autoridad vasca deba tramitar una reclamación formulada por la persona interesada, o hacer uso de sus facultades de investigación y, en su caso, sanción, bien de oficio o bien por haberse solicitado su tramitación por otra autoridad de control, tanto del Estado como de otro Estado miembro, de conformidad con las normas de procedimiento establecidas en el Reglamento General de Protección de Datos.

II

Esta ley consta de cuarenta y dos artículos, estructurados en cuatro capítulos, tres disposiciones adicionales, tres disposiciones transitorias, una disposición derogatoria y una disposición final.

El objeto de esta ley es adaptar la normativa autonómica vasca en materia de protección de datos al Reglamento (UE) 2016/679, a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como a la Ley

Orgánica 7/2021 de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, estableciendo, en particular, el régimen jurídico de la Autoridad Vasca de Protección de Datos.

La delimitación del ámbito de aplicación subjetivo de la ley se lleva a cabo a partir de la pertenencia al sector público de las entidades que tienen la condición de responsables del tratamiento o la vinculación del mencionado tratamiento con el ejercicio de potestades jurídico-públicas, a fin de regular la totalidad de los tratamientos de datos llevados a cabo por el denominado sector público.

En su ámbito de aplicación también se incluyen los tratamientos de los que sean responsables aquellas instituciones reguladas por el Estatuto de Autonomía, tales como el Parlamento Vasco, las juntas generales de los territorios históricos, el Tribunal Vasco de Cuentas Públicas y el Ararteko, así como las entidades creadas por ley del Parlamento Vasco y las autoridades administrativas independientes. Igualmente incluye a los grupos parlamentarios del Parlamento Vasco, los grupos junteros de las juntas generales de los territorios históricos y los grupos políticos municipales, así como a la Universidad del País Vasco (UPV/EHU) y las demás universidades integrantes del Sistema Universitario Vasco, así como los entes de ellas dependientes.

Así mismo, están sometidos al ámbito de competencia de la Autoridad Vasca de Protección de Datos la totalidad de los tratamientos de los que sean responsables las corporaciones de derecho público, representativas de intereses económicos y profesionales.

Por último, en relación con el sector privado, es preciso diferenciar tres supuestos de sometimiento a las disposiciones de la ley. En primer lugar, somete a su ámbito de aplicación a las personas físicas o jurídicas, si el tratamiento se lleva a cabo para el ejercicio de funciones públicas en materias que sean competencia de las administraciones públicas que integran el sector público. En segundo lugar, quedan sometidas a lo dispuesto en la norma las entidades de derecho privado que prestan servicios públicos mediante cualquier forma de gestión directa o indirecta, en lo que respecta a los tratamientos cuya finalidad se encuentre vinculada a la prestación de dichos servicios, al considerarse esos servicios como prestados por la administración titular de la competencia para su gestión. Por último, no debe olvidarse que existen entidades de derecho privado que prestan sus servicios como encargados del tratamiento a las administraciones y entidades del sector público. Estas entidades quedarán sometidas a la competencia de la Autoridad Vasca de Protección de Datos, al estar sujeta a esta última la actividad de la administración o entidad responsable del tratamiento.

Junto con el ámbito de aplicación subjetivo, en cuanto a los responsables o encargados cuya actividad queda sometida a la ley, es preciso igualmente delimitar los supuestos excluidos de su aplicación, quedando exclusivamente limitados a aquellos tratamientos referidos a personas fallecidas y los sometidos a la normativa sobre protección de materias clasificadas.

III

El capítulo II de la ley, estructurado en seis secciones, establece el régimen jurídico de la Autoridad Vasca de Protección de Datos, que sustituirá, como se indica en la disposición adicional segunda, a la actual Agencia Vasca de Protección de Datos. Se produce así un cambio esencial en la organización institucional en materia de protección de datos, que no solo afecta a la denominación de la Autoridad, sino también a su régimen jurídico, organización y competencias, desarrollando así el elenco establecido por el Reglamento (UE) 2016/679.

La sección 1.ª tiene por objeto establecer el régimen jurídico al que se somete la Autoridad Vasca de Protección de Datos, partiendo del requisito esencial de independencia con que se inviste a la autoridad de control para evitar que la injerencia de los poderes públicos afecte al adecuado cumplimiento de las funciones y potestades que tiene encomendadas. Esta independencia no solo implica el no sometimiento a instrucción alguna en el desempeño de sus competencias, sino que se materializa en la necesidad de que se la dote de los medios personales, materiales, técnicos y financieros necesarios para el cumplimiento efectivo de sus funciones.

En lo que afecta a las competencias de la Autoridad Vasca de Protección de Datos, en caso de que la doctrina emanada de ella en el ejercicio de sus funciones y potestades no pudiera ser accesible por la ciudadanía y por aquellas entidades sometidas a su competencia, el alcance del conocimiento del derecho fundamental a la protección de datos personales quedaría enormemente limitado, lo que implicaría una merma de las garantías que habrían de ser adoptadas para su protección. La ley es particularmente sensible a este necesario esfuerzo en materia de transparencia, estableciendo una serie de obligaciones adicionales a las legalmente establecidas en lo que respecta a sus obligaciones de publicidad activa.

En todo caso, la publicidad de sus resoluciones, dictámenes y documentos no puede ser ajena al propio derecho fundamental tutelado. Por este motivo, la ley prevé que, como ya es norma en otros ámbitos, como el de la publicidad de las resoluciones judiciales, se proceda, con carácter previo a llevarla a cabo, a la disociación de los datos personales que dichos documentos incorporen.

En la sección 2.ª se regulan los órganos de la Autoridad Vasca de Protección de Datos. Se opta por el mantenimiento del modelo unipersonal que ha demostrado su efectividad en los más de quince años de funcionamiento de la Agencia Vasca de Protección de Datos y que, además, se corresponde con el modelo existente en las restantes autoridades de protección de datos creadas en el Estado. Este órgano será asesorado por un consejo consultivo sin potestades ejecutivas, cuya opinión podrá ser recabada en todas las cuestiones que resulten relevantes para el adecuado ejercicio de sus competencias.

Se modifica la denominación del órgano ejecutivo de la Autoridad, que pasa a denominarse presidencia, clarificándose así su rango. Con la finalidad de reforzar su independencia, se diseña un nuevo procedimiento para su designación, en el que intervendrán el Poder ejecutivo y el legislativo. A su vez, se limitan los supuestos en que será posible el cese de quien ostente la presidencia de la Autoridad, exigiendo además la intervención del Parlamento Vasco en todos los que no se produzcan a petición propia o por la existencia de una condena penal.

El plazo de duración del mandato de la presidencia de la Autoridad se fija en cinco años, garantizándose así que no se produzca una coincidencia con la duración temporal de la legislatura, lo que sirve asimismo para reforzar la independencia de la institución y la necesidad de que concurra un consenso en su nombramiento.

Finalmente, se refuerza la consideración de la presidencia de la Autoridad, que será un alto cargo, asimilado al de las personas titulares de las viceconsejerías. No obstante, esta asimilación únicamente será aplicable a partir del primer nombramiento para la presidencia que tenga lugar con posterioridad a la entrada en vigor de la ley.

En la sección 3.ª se recalcan las competencias de investigación de la Autoridad, al ser estas las que requieren una mayor atención, en tanto permiten la adopción de medidas proactivas encaminadas a la protección del derecho y, en caso de que se haya producido su vulneración, de medidas de tipo reactivo, mediante el ejercicio de las potestades sancionadoras. Se reconoce el derecho de la Autoridad a ejercer las potestades de investigación, realizando a tal efecto inspecciones periódicas o circunstanciales, de oficio o a instancia de las personas afectadas, y en relación con cualesquiera tratamientos sometidos a su competencia, pudiendo incluso desarrollar planes de auditoría.

Al igual que en el ámbito de otras normas reguladoras de las potestades de investigación de las administraciones públicas, tales como el tributario, se establece un deber general de colaboración con la Autoridad, a la que deberán facilitarse los datos, informes, antecedentes y justificantes que fueren necesarios para llevar a cabo la actividad de investigación en el ámbito de sus competencias. En particular, se hace referencia al deber de colaboración de las haciendas forales. En todo caso, quedan excluidos los datos que fueran exclusivamente conservados por los operadores de telecomunicaciones para el cumplimiento de las obligaciones contenidas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Por su carácter novedoso, se hace especial referencia a las competencias de carácter regulatorio, a las que se dedica la sección 4.ª Así, la Autoridad, a través de su presidencia, como órgano ejecutivo, podrá dictar circulares en las que, en relación con los tratamientos sometidos a su competencia, se fijen los criterios a que responderá la actuación de esta

autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y la restante normativa de protección de datos personales que resulte de aplicación, siendo dichas circulares de obligado cumplimiento, una vez se proceda a su publicación en el «Boletín Oficial del País Vasco».

En la sección 5.ª se regula otra serie de funciones muy diversas de la Autoridad Vasca de Protección de Datos, tales como su participación como sujeto de la acción exterior y en lo que atañe a la posible celebración de acuerdos internacionales administrativos en ejecución y concreción de los tratados internacionales que así lo prevean y se refieran a materias de su competencia; los supuestos en los que su intervención será necesaria en relación con las transferencias internacionales de datos; reconoce su competencia para la aprobación de los códigos de conducta que regulen las actividades de tratamiento de los sujetos sometidos al ámbito de aplicación de la ley, así como para acreditar a organismos o entidades de certificación en materia de protección de datos respecto de las actividades de tratamiento llevadas a cabo por los responsables y encargados sometidos a su ámbito de aplicación; y, por último, la formación en protección de datos personales, por cuanto la Autoridad Vasca de Protección de Datos promoverá la difusión de las disposiciones contenidas en la normativa de protección de datos personales, con la finalidad de garantizar el adecuado conocimiento por la ciudadanía de su derecho fundamental a la protección de tales datos, y por los responsables de las obligaciones que las citadas normas les imponen para respetarlo.

Por último, la sección 6.ª establece los aspectos esenciales de la relación de la Autoridad Vasca de Protección de Datos con las restantes autoridades de protección de datos del Estado. Profundiza en el reconocimiento del principio de cooperación institucional entre las autoridades de protección de datos del Estado, poniendo de manifiesto su esencial vinculación con la propia razón de ser de las autoridades de control, dado que con la garantía de su adecuada cooperación, colaboración y coordinación se logra el objetivo de garantizar la adecuada protección del derecho fundamental a la protección de datos personales. En este sentido, se prevé la potestad de la Autoridad Vasca de Protección de Datos de suscribir con las restantes autoridades de protección de datos del Estado los protocolos, acuerdos y convenios de colaboración que fuesen necesarios para el adecuado desarrollo de la cooperación institucional.

Se reconoce a su vez la importancia de las actuaciones conjuntas de investigación y la posibilidad de desarrollar planes conjuntos de auditoría, así como los supuestos de cooperación en el marco de los procedimientos transfronterizos.

IV

El capítulo III de la ley regula el régimen sancionador, al que quedan sometidos los responsables y encargados de los tratamientos sometidos a su ámbito de aplicación, así como las entidades acreditadas de supervisión de los códigos de conducta aprobados por la Autoridad Vasca de Protección de Datos, y las entidades de certificación acreditadas por dicha autoridad.

Una de las principales novedades que introduce el Reglamento General de Protección de Datos es el establecimiento de un marco sancionador uniforme para la reacción ante las vulneraciones en materia de protección de datos en el ámbito de toda la Unión Europea. De este modo, es el propio reglamento el que determina las conductas típicas constitutivas de infracción y el régimen sancionador aplicable en caso de comisión de las conductas típicas.

Al propio tiempo, estas disposiciones se complementan por la normativa interna de los estados miembros, que en el ámbito estatal está constituida por las concretas previsiones contenidas en los artículos, que se citan, de las leyes orgánicas a las que, atendiendo a su objeto, la presente ley adapta la normativa autonómica vasca en materia de protección de datos.

La ley establece una clara diferenciación entre el régimen sancionador aplicable al sector público y al privado. Por lo que a este último se refiere, para las infracciones contempladas en la ley se prevén diversas sanciones de multa, así como los criterios para la graduación de su importe, que se impondrán en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas establecidas en el Reglamento (UE) 2016/679.

De otro lado, la comisión de alguna de las infracciones a las que se refiere esta ley, por las administraciones, entidades e instituciones públicas vascas incluidas en su ámbito de

aplicación, cuando actúen como responsables o encargados del tratamiento, no será sancionada con la imposición de una sanción económica, sino con apercibimiento, con indicación de las medidas correctivas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

Se establece igualmente la adopción de medidas específicas en los supuestos en los que las infracciones fueran imputables a autoridades, altos cargos y personal directivo, y se hubiera acreditado que la acción infractora se llevó a cabo en contra del criterio sustentado por informes técnicos o recomendaciones para el tratamiento, que no hubieran sido debidamente atendidos. En este caso, se prevé expresamente que en la resolución en la que se imponga la sanción se incluirá una amonestación con la denominación del cargo que fuese responsable y se ordenará su publicación en el «Boletín Oficial del País Vasco».

Finalmente, y como especialidades propias del régimen del sector público en la Comunidad Autónoma del País Vasco, se prevé que, junto con las medidas establecidas con carácter general, será aplicable lo establecido en el Código Ético y de Conducta de los cargos públicos y personal eventual de la Administración General e Institucional de la Comunidad Autónoma del País Vasco, así como que se comunicarán al Ararteko las resoluciones sancionadoras que se dicten.

En este concreto apartado, el principio de transparencia exige garantizar el adecuado escrutinio de la actividad pública, garantizando el público conocimiento del modo en que se lleva a cabo, de forma que sea de público conocimiento la existencia de cualquier desviación que pudiera haberse producido en la mencionada gestión.

Por este motivo, se regula expresamente un régimen especial de publicidad en el ámbito del sector público, que permita a la ciudadanía conocer el efectivo cumplimiento de la normativa por los entes y organismos que lo integran o por quienes, incardinados en el sector privado, tienen a su cargo la ejecución de esta actividad.

En este sentido, se prevé la publicación en el «Boletín Oficial del País Vasco» de la información relevante referida a las sanciones de mayor gravedad impuestas por la Autoridad Vasca de Protección de Datos, limitando los datos publicados a la información que identifique a la persona infractora, la infracción cometida y el importe de la sanción impuesta cuando exceda de un millón de euros y la persona infractora sea una persona jurídica; y a las amonestaciones impuestas a las autoridades, altos cargos y personal directivo que hubieran ordenado la realización de la conducta infractora apartándose para ello de informes técnicos o recomendaciones para el tratamiento de los datos.

Por último, y por lo que se refiere a la prescripción de las sanciones, la ley opta por el mantenimiento de los plazos de prescripción que ya regían con anterioridad a la entrada en vigor del Reglamento (UE) 2016/679, estableciendo los plazos en función de las cuantías que en el anterior marco normativo se preveían para las infracciones por sanciones leves, graves y muy graves. Además, y en coherencia con su objeto, que contempla la adaptación de la normativa autonómica vasca a las previsiones contenidas en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, se regulan también los plazos de prescripción de las sanciones contempladas en dicha ley, en función de su importe.

V

El capítulo IV, compuesto por cinco secciones, regula los procedimientos en caso de infracción de las normas de protección de datos.

La sección 1.ª, disposiciones generales, regula el régimen jurídico aplicable y las causas de suspensión del procedimiento.

Como punto de partida, la ley delimita el alcance de la aplicación de las normas que contiene, que no son de aplicación a todos los procedimientos tramitados por la Autoridad Vasca de Protección de Datos, sino únicamente a aquellos en los que resulta necesario el establecimiento de especialidades respecto de lo establecido en la normativa general reguladora del procedimiento administrativo. De este modo, se regulan los tres supuestos en los que serán de aplicación las normas contenidas en este capítulo, siendo de aplicación subsidiaria a los procedimientos sancionadores lo establecido en la normativa reguladora del

ejercicio de la potestad sancionadora de las administraciones públicas de la Comunidad Autónoma del País Vasco.

El efecto suspensivo del procedimiento se prevé no solo en los casos previstos en la normativa básica, sino también en aquellos en los que deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de otras autoridades de control. Esta suspensión se extendería durante el período que media entre la solicitud y la notificación del pronunciamiento a la Autoridad Vasca de Protección de Datos.

La sección 2.ª regula la iniciación del procedimiento, que incluye la admisión a trámite de la reclamación y las actuaciones previas que han de llevarse a cabo, tal como el análisis de la competencia de la autoridad de control, incorporándose la posibilidad de la adopción de una decisión acerca de la procedencia o no de la tramitación del procedimiento. A tal efecto, enumera una serie de supuestos en los que no procedería proseguir con el procedimiento, sino acordar su inadmisión.

Se prevé a su vez que la Autoridad Vasca de Protección de Datos puede acordar de oficio el inicio del procedimiento al tener conocimiento de la existencia de indicios de la comisión de una infracción de lo dispuesto en la normativa de protección de datos personales. Igualmente, es posible que la iniciación se deba al requerimiento de otra autoridad de protección de datos, tanto del Estado como de otro Estado miembro.

Las secciones 3.ª y 4.ª regulan, respectivamente, la tramitación del procedimiento en caso de reclamaciones derivadas del ejercicio de derechos, y del procedimiento de ejercicio de la potestad sancionadora.

La ley diferencia, siguiendo el criterio ya existente en la normativa actualmente vigente, entre los procedimientos relacionados exclusivamente con el reconocimiento del ejercicio por las personas interesadas de los derechos consagrados por las normas de protección de datos, y los procedimientos relacionados con el ejercicio de la potestad sancionadora. Lógicamente, en los supuestos en los que la reclamación formulada por la persona interesada contuviese ambas pretensiones, la Autoridad Vasca de Protección de Datos podrá decidir la apertura de dos procedimientos diferenciados.

La diferencia es sustancial, dado que se pretende que el procedimiento relacionado con la atención de los derechos, que en la mayor parte de los supuestos se centrará en la cuestión de valoración de la prueba de que los derechos fueron atendidos o, a lo sumo, en la improcedencia de dicha atención, tenga una duración sustancialmente inferior a la de los procedimientos sancionadores, en los que, además, será posible la adopción de medidas cautelares que garanticen un rápido restablecimiento del derecho cuando así proceda.

En relación con los procedimientos referidos a la solicitud no atendida de ejercicio de derechos, la ley mantiene el principio contradictorio, estableciendo un plazo máximo de resolución del procedimiento de seis meses, tras los cuales la persona interesada podrá considerar desestimada su reclamación.

Por último, la sección 5.ª regula las diferentes especialidades en los casos de procedimientos referidos a tratamientos transfronterizos. La ley adopta las medidas normativas pertinentes para tener en cuenta las nuevas situaciones introducidas por el reglamento europeo de protección de datos. En concreto, introduce especialidades en los supuestos en los que varias autoridades de protección de datos pudieran tener interés en la resolución del procedimiento, diferenciando entre la autoridad principal, en cuya jurisdicción esté ubicado el establecimiento principal del responsable, de las restantes autoridades interesadas.

VI

La ley contiene tres disposiciones adicionales, tres disposiciones transitorias, una disposición derogatoria y una disposición final.

La disposición adicional primera comprende la referencia de la normativa aplicable a los procedimientos tramitados por la Autoridad Vasca de Protección de Datos no regulados por esta ley, en los que su actividad quedará plenamente sometida a la legislación básica y autonómica reguladora del procedimiento administrativo.

La disposición adicional segunda especifica que la Autoridad Vasca de Protección de Datos reemplaza a la Agencia Vasca de Protección de Datos, asumiendo las competencias y las funciones de supervisión, control, asesoramiento o informe, entre otras, que se le

hubieran venido atribuyendo por la normativa actualmente vigente, por lo que las referencias a la Agencia deberán entenderse llevadas a cabo a la Autoridad.

La disposición adicional tercera establece la creación de cuerpos y escalas de personal funcionario propio de la Autoridad Vasca de Protección de Datos, conforme a la normativa de aplicación, incluyéndose cuestiones relativas a la relación de puestos de trabajo, el acceso de personal funcionario propio y de personal procedente de otras administraciones, así como la posibilidad de llevar a cabo un sistema de equivalencias entre cuerpos y escalas propios y aquellos de otras administraciones públicas.

La disposición transitoria primera aclara que el nuevo régimen de la Autoridad Vasca de Protección de Datos exigirá la adopción de un nuevo estatuto, que sustituya al actualmente vigente. Sin embargo, sus especialidades pueden ser perfectamente aplicables, en cuanto no se opongan a lo establecido en la ley, mientras no se proceda a la aprobación de ese nuevo estatuto. Al propio tiempo, se clarifica que la asimilación de la presidencia de la Autoridad Vasca de Protección de Datos al cargo de viceconsejero o viceconsejera y la nueva composición del consejo consultivo se producirán cuando proceda la realización de una nueva designación de los mismos, sin que la entrada en vigor de esta ley pueda implicar el cese de quien ostente el puesto de director o directora de la Agencia Vasca de Protección de Datos ni de quienes conformen su consejo consultivo.

La disposición transitoria segunda está dedicada al régimen transitorio de los procedimientos, de forma que las actuaciones previas de investigación y los procedimientos iniciados con anterioridad a la entrada en vigor de esta ley continuarán tramitándose de conformidad con la normativa aplicable en el momento de su inicio.

La disposición transitoria tercera establece el sistema de integración del personal funcionario de la Agencia Vasca de Protección de Datos en los cuerpos y escalas del personal funcionario de la Autoridad Vasca de Protección de Datos. Se diferencian tres supuestos: el personal consolidado como consecuencia de los procesos de estabilización excepcional convocados previamente; el personal funcionario de carrera procedente de otras administraciones públicas, y el personal que ocupa puestos en régimen de comisión de servicios o como personal funcionario interino.

La disposición derogatoria única señala las normas que quedan derogadas a la entrada en vigor de la presente ley: la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, el Decreto 308/2005, de 18 de octubre, por el que se desarrolla la ley anteriormente mencionada, y el Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos.

Por último, la disposición final se refiere a la entrada en vigor de esta ley.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. La presente ley tiene por objeto regular el control y supervisión de los tratamientos de datos de los que sean responsables los sujetos incluidos en su ámbito de aplicación.

2. Asimismo, la presente ley tiene por objeto regular el régimen jurídico de la Autoridad Vasca de Protección de Datos.

Artículo 2. *Ámbito de aplicación.*

1. La presente ley será de aplicación a todos los tratamientos de datos personales de los que sean responsables:

a) La Administración general de la Comunidad Autónoma del País Vasco, las administraciones forales de los territorios históricos y las administraciones locales del ámbito territorial de la Comunidad Autónoma del País Vasco, así como sus correspondientes administraciones institucionales y los entes integrantes de su respectivo sector público.

b) Los entes integrantes del sector público previstos en los apartados 3 y 4 del artículo 4 de la Ley 3/2022, de 12 de mayo, del Sector Público Vasco.

c) El Parlamento Vasco.

d) Las juntas generales de los territorios históricos.

e) El Tribunal Vasco de Cuentas Públicas.

f) El Ararteko.

g) Las entidades creadas por ley del Parlamento Vasco y las autoridades administrativas independientes.

h) Los grupos parlamentarios del Parlamento Vasco, los grupos junteros de las juntas generales de los territorios históricos y los grupos municipales de los ayuntamientos.

i) Las corporaciones de derecho público, representativas de intereses económicos y profesionales, cuyo ámbito territorial no exceda de la Comunidad Autónoma del País Vasco, así como las delegaciones de dichas corporaciones que, actuando con plena autonomía orgánica, funcional y económica para la realización de los fines, tuviesen un ámbito territorial que no excediera de dicha comunidad autónoma.

j) La Universidad del País Vasco (UPV/EHU) y las demás universidades integrantes del Sistema Universitario Vasco, así como los entes de ellas dependientes.

k) Consejo de Relaciones Laborales y Consejo Económico y Social Vasco.

l) Las personas físicas o jurídicas, si el tratamiento se lleva a cabo para el ejercicio de funciones públicas en materias que sean competencia de las administraciones públicas enumeradas en la letra a).

m) Las entidades de derecho privado que prestan servicios públicos mediante cualquier forma de gestión directa o indirecta, en lo que respecta a los tratamientos cuya finalidad se encuentre vinculada a la prestación de dichos servicios.

2. Estarán igualmente sometidos a lo dispuesto en la presente ley las personas físicas o jurídicas, públicas o privadas que, como encargados del tratamiento, presten servicios a los responsables a los que se refieren el apartado 1 de este artículo.

3. La presente ley no se aplicará a:

a) Los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 3 de la Ley Orgánica 7/2021, de 26 de mayo.

b) Los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

CAPÍTULO II

La Autoridad Vasca de Protección de Datos

Sección 1.ª Organización y régimen jurídico

Artículo 3. *Naturaleza y régimen jurídico.*

1. La Autoridad Vasca de Protección de Datos es una autoridad administrativa independiente, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones.

La Autoridad Vasca de Protección de Datos se relaciona con el Gobierno Vasco a través del departamento que determine el lehendakari o la lehendakari en el decreto de áreas.

2. La Autoridad Vasca de Protección de Datos tiene la condición de autoridad de control independiente a los efectos de lo dispuesto en el capítulo VI del Reglamento (UE) 2016/679 y en el capítulo VI de la Ley Orgánica 7/2021, de 26 de mayo.

3. Los procedimientos tramitados por la Autoridad Vasca de Protección de Datos en el ejercicio de sus potestades de supervisión y control se someterán a la presente ley y a su normativa de desarrollo y, supletoriamente, cuando dichos procedimientos revistan carácter sancionador, a lo establecido en la normativa reguladora de la potestad sancionadora de las administraciones públicas de la Comunidad Autónoma del País Vasco.

4. La representación y defensa en juicio de la Autoridad Vasca de Protección de Datos estará a cargo del Servicio Jurídico Central del Gobierno Vasco, conforme a lo dispuesto en sus normas reguladoras, siempre que no existan intereses contrapuestos con las

administraciones u organismos públicos cuya representación legal o convencional ostente el Servicio Jurídico Central del Gobierno Vasco.

5. Corresponde al Gobierno Vasco aprobar el Estatuto de la Autoridad Vasca de Protección de Datos, así como dictar cuantas disposiciones reglamentarias sean precisas para el desarrollo de la presente ley.

Artículo 4. *Régimen económico y presupuestario.*

1. La Autoridad Vasca de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto, y lo remitirá al Gobierno Vasco para que sea integrado, con la debida independencia, en los presupuestos generales de la Comunidad Autónoma, de acuerdo con la legislación reguladora del régimen presupuestario de la Comunidad Autónoma del País Vasco. Estará sometida a dicha legislación en lo relativo al régimen de modificación, ejecución y liquidación de su presupuesto, atendiendo a estos efectos a la naturaleza de la Autoridad.

2. La Autoridad Vasca de Protección de Datos contará con recursos suficientes para el desempeño de sus funciones y ejercicio de sus potestades. Dichos recursos procederán de:

a) Las asignaciones que se establezcan con cargo a los presupuestos generales de la Comunidad Autónoma.

b) Las subvenciones y aportaciones que se concedan a su favor.

c) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

d) Los ingresos, ordinarios y extraordinarios, derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidas en el artículo 58 del Reglamento (UE) 2016/679, y en el artículo 50 de la Ley Orgánica 7/2021, de 26 de mayo.

e) Cualesquiera otros que legalmente le pudieran ser atribuidos.

3. Los ingresos procedentes o derivados del ejercicio de las actividades y potestades que la presente ley atribuye a la Autoridad Vasca de Protección de Datos se destinarán por esta a la dotación de sus reservas.

4. La Autoridad Vasca de Protección de Datos estará sometida al control económico-financiero y de gestión de la Comunidad Autónoma del País Vasco, así como a la fiscalización del Tribunal Vasco de Cuentas Públicas.

Artículo 5. *Régimen de personal.*

1. El personal al servicio de la Autoridad Vasca de Protección de Datos será funcionario, y se regirá por la legislación reguladora de la función pública vasca.

2. La relación de puestos de trabajo de la Autoridad Vasca de Protección de Datos será aprobada por resolución de su presidencia y entrará en vigor el día de su publicación en el «Boletín Oficial del País Vasco».

3. Corresponde a la Autoridad Vasca de Protección de Datos determinar el régimen de acceso a sus puestos de trabajo, los requisitos y las características de las pruebas de selección, así como la convocatoria, gestión y resolución de los procedimientos de provisión de puestos de trabajo y promoción profesional.

4. El personal de la Autoridad Vasca de Protección de Datos estará obligado a guardar secreto sobre las informaciones que conozca en el ejercicio de sus funciones, incluso después de haber cesado en estas.

Artículo 6. *Funciones y potestades.*

La Autoridad Vasca de Protección de Datos ejercerá las funciones establecidas y las potestades previstas, respectivamente, en los artículos 57 y 58 del Reglamento (UE) 2016/679, en los artículos 49 y 50 de la Ley Orgánica 7/2021, de 26 de mayo, así como las previstas en esta ley.

Asimismo, ejercerá cuantas competencias le sean legalmente atribuidas.

Artículo 7. *Transparencia.*

1. Además de cumplir las exigencias establecidas en la normativa aplicable en materia de transparencia y acceso a la información pública, la Autoridad Vasca de Protección de Datos hará públicas a través de su página web las resoluciones de su presidencia que pongan término a los procedimientos relacionados con la vulneración de las disposiciones de protección de datos o con la atención de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como aquellas por las que se adopten cláusulas contractuales tipo para las transferencias internacionales de datos, se autoricen transferencias internacionales de datos, o se acrediten entidades de certificación.

2. También hará públicas a través de su página web las resoluciones de su presidencia que pongan término a los procedimientos relacionados con la vulneración de las disposiciones de protección de datos, o con la atención de los derechos establecidos en los artículos 21, 22 y 23 de la Ley Orgánica 7/2021, de 26 de mayo.

Cuando las resoluciones a las que se refiere el párrafo anterior traigan su causa de lo establecido en un dictamen del Comité Europeo de Protección de Datos, este será objeto de publicación junto con la resolución adoptada.

3. Además, la Autoridad Vasca de Protección de Datos hará públicas a través de su página web:

a) Las directrices generales que se adopten como consecuencia de la realización de planes de auditoría.

b) Los informes preceptivos a disposiciones de carácter general evacuados conforme al apartado 4 del artículo 36 del Reglamento (UE) 2016/679.

c) Los dictámenes por los que se dé respuesta a consultas que le hayan sido planteadas, en la medida en que supongan una interpretación de las normas de protección de datos que no haya sido previamente objeto de publicación.

d) Los códigos de conducta aprobados por la Autoridad.

e) Las restantes actuaciones que hayan de hacerse públicas conforme a la normativa de protección de datos personales.

4. La difusión a la que se refieren los apartados anteriores se llevará a cabo previa disociación de los datos de carácter personal y respetando los límites establecidos en la legislación aplicable en materia de transparencia y acceso a la información pública.

Sección 2.ª Órganos de la Autoridad Vasca de Protección de Datos

Artículo 8. *Presidencia de la Autoridad Vasca de Protección de Datos.*

1. La presidencia de la Autoridad Vasca de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

Los actos de la autoridad vasca que produzcan efectos jurídicos sobre terceros serán dictados por su presidencia.

2. La presidencia de la Autoridad Vasca de Protección de Datos ejercerá sus funciones con plena independencia y objetividad, y no estará sujeta a instrucción alguna en el desempeño de aquellas.

3. La presidencia de la Autoridad Vasca de Protección de Datos será nombrada por decreto del Gobierno Vasco por un período de cinco años, pudiendo ser renovada por un único período de igual duración.

A tal efecto, el Gobierno Vasco propondrá al Parlamento Vasco la persona que considere idónea para presidir la Autoridad Vasca de Protección de Datos. Dicha persona poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

4. Recibida la propuesta por el Parlamento Vasco, se someterá a la comisión competente, que deberá aprobarla por mayoría absoluta. En caso de no obtenerse dicha mayoría se entenderá decaída la propuesta, y se devolverá al Gobierno Vasco.

5. La presidencia de la Autoridad Vasca de Protección de Datos solo cesará antes de la expiración de su mandato por alguna de las siguientes causas:

a) A petición propia.

b) Por condena firme por delito doloso.
c) Por incumplimiento grave de sus obligaciones.
d) Por incapacidad sobrevenida para el ejercicio de su función.
e) Por incompatibilidad.

En los supuestos previstos en las letras c), d) y e) será necesaria la ratificación de la separación por mayoría absoluta de la Comisión de Instituciones, Gobernanza Pública y Seguridad del Parlamento Vasco.

6. La presidencia de la Autoridad Vasca de Protección de Datos tendrá la consideración de alto cargo, asimilado al de viceconsejero o viceconsejera. Si con anterioridad a su nombramiento estuviera ocupando una plaza como funcionaria o funcionario público, quedará en situación de servicios especiales.

En todo caso, le será de aplicación lo dispuesto en la Ley 1/2014, de 26 de junio, Reguladora del Código de Conducta y de los Conflictos de Intereses de los Cargos Públicos y su normativa de desarrollo.

7. Los actos y disposiciones dictados por la presidencia de la Autoridad Vasca de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la jurisdicción contencioso-administrativa.

8. La presidencia de la Autoridad Vasca de Protección de Datos, de conformidad con lo dispuesto en el artículo 59 del Reglamento General de Protección de Datos, elaborará un informe anual de sus actividades, que será comunicado al Parlamento Vasco, al Gobierno Vasco y a las demás autoridades de protección de datos del Estado. Este informe será publicado en su página web.

Artículo 9. *El Consejo Consultivo de la Autoridad Vasca de Protección de Datos.*

1. La presidencia de la Autoridad Vasca de Protección de Datos estará asesorada por un consejo consultivo compuesto por los siguientes miembros:

a) Una persona representante del Parlamento Vasco, designada por este.
b) Una persona representante de la Administración general de la Comunidad Autónoma del País Vasco, designada por el Gobierno Vasco.
c) Una persona representante de cada uno de los territorios históricos vascos, designada por estos.
d) Una persona representante de las entidades locales del ámbito territorial de la Comunidad Autónoma del País Vasco, designada por la Asociación de Municipios Vascos.
e) Una persona representante de las personas consumidoras y usuarias, designada por Kontsumobide-Instituto Vasco de Consumo.
f) Dos personas expertas, una en tecnologías de la información y otra en el ámbito del Derecho, con conocimientos acreditados en el Derecho y la práctica en materia de protección de datos, designadas de forma rotatoria por las universidades del Sistema Universitario Vasco.
g) Una persona experta designada por Cyberzaintza, Agencia Vasca de Ciberseguridad.

2. Se procurará que la composición del consejo consultivo tenga una representación equilibrada entre mujeres y hombres, con capacitación, competencia y preparación adecuada. A los efectos, se considera representación equilibrada cuando ambos sexos estén representados al menos al 40 %.

3. El consejo consultivo se reunirá cuando así lo disponga la presidencia de la Autoridad Vasca de Protección de Datos y, en todo caso, una vez al semestre.

4. Los acuerdos adoptados por el consejo consultivo no tendrán en ningún caso carácter vinculante. No obstante, será preceptiva la emisión de informe del consejo consultivo previo a la aprobación de circulares interpretativas de la ley y normativa de desarrollo que, en el ejercicio de la potestad normativa a la que alude el artículo 15 de esta ley, tiene atribuida la presidencia, sin perjuicio de que, igualmente, dichos informes carezcan de carácter vinculante.

5. En lo no previsto en este artículo, el régimen, organización, competencias y funcionamiento del consejo consultivo se regulará por el Estatuto de la Autoridad Vasca de Protección de Datos.

Sección 3.ª Potestad de investigación

Artículo 10. *Ámbito de la potestad de investigación.*

1. La Autoridad Vasca de Protección de Datos podrá, en ejercicio de sus potestades de investigación, realizar inspecciones periódicas o circunstanciales, de oficio o a instancia de las personas afectadas, de cualquiera de los tratamientos sometidos al ámbito de aplicación de esta ley.

2. Asimismo, podrá desarrollar las citadas funciones con ocasión de la realización de un plan de auditoría, en los términos establecidos en el artículo 14 de la presente ley.

Artículo 11. *Personal competente para realizar la actividad de investigación.*

1. La actividad de investigación se llevará a cabo por el personal inspector de la Autoridad Vasca de Protección de Datos.

2. No obstante, la presidencia de la Autoridad Vasca de Protección de Datos podrá habilitar expresamente a otro personal funcionario público para la realización de actividades de investigación. La habilitación indicará las actividades concretas de investigación a las que la misma se circunscribe.

3. En los supuestos de actuaciones conjuntas de investigación conforme a lo dispuesto en el artículo 62 del Reglamento (UE) 2016/679, el personal de las autoridades de control de otros estados miembros de Unión Europea que colabore con la Autoridad Vasca de Protección de Datos ejercerá sus facultades con arreglo a lo previsto en la presente ley. Dicho personal actuará en presencia del personal de la Autoridad Vasca de Protección de Datos y bajo su orientación y dirección.

4. El personal funcionario que desarrolle actividades de investigación tendrá a todos los efectos la condición de agente de la Autoridad Vasca de Protección de Datos en el ejercicio de sus funciones.

Artículo 12. *Alcance de la actividad de investigación.*

1. Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones. En particular, podrán:

a) Acceder a los locales en que se encuentren los sistemas de información o se lleven materialmente a cabo los tratamientos de datos.

b) Examinar los soportes de información que contengan los datos personales y obtener copia de los datos sometidos a tratamiento.

c) Examinar, en el lugar en que se encuentren, los sistemas de información que traten datos personales, incluyendo los equipos físicos y lógicos en que se lleve a cabo el tratamiento.

d) Requerir el envío de los programas y aplicaciones o de la documentación pertinente, a fin de analizar el tratamiento del que sean objeto los datos, y obtener copia de ellos.

e) Requerir la ejecución de los programas, aplicaciones o procedimientos de gestión y soporte del tratamiento que se encuentren sujetos a investigación.

f) Realizar auditorías de los sistemas de información, sistemas de decisión individual automatizada, sistemas de inteligencia artificial y sistemas algorítmicos, y de dispositivos, equipos o programas que faciliten el tratamiento de los datos, a fin de determinar su conformidad o no con la legislación vigente.

g) Requerir la exhibición o remisión de cualquier otra información que resulte precisa para el ejercicio de las funciones inspectoras.

h) Revisar las medidas técnicas y organizativas adoptadas en relación con los tratamientos.

2. Cuando fuese necesario el acceso por el personal que desarrolla la actividad de investigación al domicilio, constitucionalmente protegido, de la persona inspeccionada, será preciso contar con su consentimiento o haber obtenido la correspondiente autorización judicial, respetando su inviolabilidad.

Artículo 13. *Deber de colaboración.*

1. Las administraciones públicas, incluidas las haciendas forales, así como las personas físicas o jurídicas, estén o no sometidos sus tratamientos a lo dispuesto en la presente ley, estarán obligados a proporcionar a la Autoridad Vasca de Protección de Datos los datos, informes, antecedentes y justificantes que fueren necesarios para llevar a cabo la actividad de investigación en el ámbito de sus competencias. Cuando la información contenga datos personales, la comunicación de dichos datos estará amparada por lo dispuesto en el artículo 6.1.c) del Reglamento (UE) 2016/679.

2. La Autoridad Vasca de Protección de Datos tendrá, en el ámbito de sus competencias, las facultades previstas en los apartados 2 y 3 del artículo 52 de la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 14. *Planes de auditoría.*

1. La presidencia de la Autoridad Vasca de Protección de Datos podrá acordar la realización de planes de auditoría, referidos bien a un determinado ámbito de responsables o encargados del tratamiento sometidos a la aplicación de la presente ley, bien a un determinado tipo de actividad de tratamiento.

2. Los planes de auditoría preventiva tendrán por objeto el análisis del cumplimiento de las disposiciones del Reglamento (UE) 2016/679 y la restante normativa en materia de protección de datos personales que resulte aplicable.

3. Como resultado de los planes de auditoría, la presidencia de la Autoridad Vasca de Protección de Datos deberá dictar las directrices que resulten precisas para asegurar el pleno cumplimiento de las normas de protección de datos. Dichas directrices podrán ir dirigidas a la totalidad de los sujetos inspeccionados, o a un responsable o encargado del tratamiento concreto.

Las directrices serán en todo caso de obligado cumplimiento.

Sección 4.ª Potestad normativa

Artículo 15. *Circulares de la Autoridad Vasca de Protección de Datos.*

1. La presidencia de la Autoridad Vasca de Protección de Datos aprobará las directrices interpretativas de esta ley y de su normativa de desarrollo, así como, en su caso, de la restante normativa de protección de datos personales que resulte de aplicación.

2. En relación con los tratamientos sometidos a la presente ley, deberá dictar las circulares que resulten precisas, en las que se fijen los criterios a los que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y la restante normativa de protección de datos personales que resulte de aplicación.

3. Para su elaboración se recabarán los informes técnicos y jurídicos que fueran necesarios, garantizando en todo caso la audiencia a las personas interesadas durante su elaboración, cuando ello fuera necesario.

4. Las circulares serán obligatorias para los sujetos sometidos a la presente ley una vez publicadas en el «Boletín Oficial del País Vasco».

Sección 5.ª Otras competencias de la Autoridad Vasca de Protección de Datos

Artículo 16. *Mecanismos de coordinación y cooperación entre autoridades de protección de datos en materias competencia de la Comunidad Autónoma del País Vasco.*

1. La Autoridad Vasca de Protección de Datos podrá, en el marco de sus competencias, ejercitar las funciones que le competen a la Comunidad Autónoma del País Vasco como sujeto de la acción exterior de conformidad con la normativa reguladora de la acción exterior del Estado.

2. La Autoridad Vasca de Protección de Datos podrá, en representación de la Comunidad Autónoma del País Vasco, celebrar acuerdos internacionales administrativos en ejecución y concreción de un tratado internacional cuando así lo prevea el propio tratado, le atribuya potestad para ello y verse sobre materias de su competencia conforme a lo dispuesto en la presente ley.

3. Asimismo, la Autoridad Vasca de Protección de Datos podrá celebrar acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, no vinculantes jurídicamente para quienes los suscriben, sobre materias de su competencia.

Artículo 17. *Transferencias internacionales de datos.*

1. La Autoridad Vasca de Protección de Datos podrá adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de datos por los responsables y encargados del tratamiento sometidos a su competencia.

2. Asimismo, podrá aprobar, en dicho ámbito, normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.

3. La Autoridad Vasca de Protección de Datos autorizará las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión Europea o que no se amparen en alguna de las garantías previstas en los apartados anteriores. La autorización podrá otorgarse:

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.

b) Cuando la transferencia se lleve a cabo por un sujeto de derecho público y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros estados, que incorporen derechos efectivos y exigibles para las personas afectadas, incluidos los memorandos de entendimiento.

4. La resolución de la Autoridad Vasca de Protección de Datos se someterá al dictamen del Comité Europeo de Protección de Datos, en los términos previstos por el artículo 64 del Reglamento (UE) 2016/679.

5. En los supuestos establecidos en los apartados 2 y 3, la solicitud del dictamen al Comité Europeo de Protección de Datos implicará la suspensión del procedimiento para resolver sobre la procedencia de la transferencia internacional solicitada, que no se levantará hasta la notificación de dicho dictamen a la Autoridad Vasca de Protección de Datos.

6. La Autoridad Vasca de Protección de Datos podrá solicitar de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia del País Vasco la autorización judicial a la que se refiere la disposición adicional quinta de la Ley Orgánica 3/2018, de 5 de diciembre.

7. Las transferencias internacionales de datos con la finalidad de prevención, detección, investigación y enjuiciamiento de infracciones penales y ejecución de sanciones penales se regirán por lo dispuesto en el capítulo V de la Ley Orgánica 7/2021, de 26 de mayo.

8. Los responsables del tratamiento deberán informar a la Autoridad Vasca de Protección de Datos de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquellos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos.

Artículo 18. *Códigos de conducta.*

1. La Autoridad Vasca de Protección de Datos promoverá y aprobará los códigos de conducta que regulen las actividades de tratamiento de los sujetos sometidos al ámbito de aplicación de la presente ley. Asimismo, deberá elaborar y publicar los criterios que resulten precisos para la acreditación de organismos de supervisión de los códigos de conducta.

2. La Autoridad Vasca de Protección de Datos someterá los proyectos de código de conducta al mecanismo de coherencia mencionado en el artículo 63 de Reglamento (UE) 2016/679, en los supuestos en que ello proceda según su artículo 40.7. El procedimiento de aprobación del código quedará suspendido en tanto el Comité Europeo de Protección de Datos no emita el dictamen al que se refieren los artículos 64.1.b) y 65.1.c) del citado reglamento.

3. La Autoridad Vasca de Protección de Datos mantendrá un registro, accesible a través de medios electrónicos, de los códigos de conducta aprobados por ella, que se

interconectará con los de las restantes autoridades de protección de datos del Estado. Asimismo, el registro se coordinará con el gestionado por el Comité Europeo de Protección de Datos conforme al artículo 40.11 del Reglamento (UE) 2016/679.

4. Mediante decreto se establecerá el contenido del registro y las especialidades del procedimiento de aprobación.

Artículo 19. *Certificaciones.*

1. La Autoridad Vasca de Protección de Datos podrá expedir certificaciones, aprobar criterios de certificación y acreditar a organismos o entidades de certificación en materia de protección de datos respecto de las actividades de tratamiento llevadas a cabo por los responsables y encargados a los que se refiere el artículo 2 de la presente ley, con arreglo a lo dispuesto en los artículos 42 y 43 del Reglamento General de Protección de Datos.

2. Sin perjuicio de lo anterior, la Entidad Nacional de Acreditación (ENAC), comunicará en todo caso a la Autoridad Vasca de Protección de Datos las concesiones, denegaciones o revocaciones de las acreditaciones de entidades de certificación que hubiera adoptado, así como la motivación en que se hubiera fundado.

Artículo 20. *Formación y sensibilización en protección de datos personales y derechos digitales.*

1. La Autoridad Vasca de Protección de Datos promoverá la difusión y formación en relación con las disposiciones contenidas en la normativa de protección de datos personales y sobre derechos digitales, con la finalidad de garantizar el adecuado conocimiento tanto por la ciudadanía como por los responsables de las obligaciones que las citadas normas les imponen para respetarlos. Se garantizará la sensibilización y formación en materia de privacidad y protección de datos en todas las esferas de la sociedad, comenzando por edades muy tempranas –a partir de los tres años–, promoviendo la privacidad y protección de datos para el alumnado y sus familias, con especial hincapié en el uso de las redes sociales.

2. A tal efecto, concluirá acuerdos y convenios de colaboración con la Universidad del País Vasco (UPV/EHU) y las restantes universidades y entidades integrantes del Sistema Universitario Vasco, así como con centros educativos no universitarios y responsables de los tratamientos, profesionales y personas consumidoras.

Sección 6.ª Cooperación con otras autoridades de protección de datos

Artículo 21. *Principio de cooperación institucional.*

1. La Autoridad Vasca de Protección de Datos garantiza el cumplimiento de los principios de cooperación, colaboración y coordinación con las restantes autoridades de protección de datos del Estado, a fin de garantizar la adecuada protección del derecho fundamental a la protección de datos personales, respetando en todo caso el principio de lealtad institucional.

2. A tal efecto, la Autoridad Vasca de Protección de Datos:

a) Facilitará a las restantes autoridades la información de que dispusiera y que aquellas precisasen para el adecuado desarrollo de sus competencias, cuando así le fuera solicitada.

b) Prestará, en el ámbito de la Comunidad Autónoma del País Vasco, la asistencia y auxilio que las restantes autoridades de protección de datos del Estado pudieran solicitar para el eficaz ejercicio de sus competencias.

c) Desarrollará, cuando así se acuerde, actuaciones comunes de auditoría e investigación.

d) Participará activamente en los grupos de trabajo que se constituyeran para tratar asuntos específicos de interés común.

3. La Autoridad Vasca de Protección de Datos podrá suscribir con las restantes autoridades de protección de datos del Estado los protocolos, acuerdos y convenios de colaboración que fuesen necesarios para el adecuado desarrollo de la cooperación institucional regulada en este artículo.

Artículo 22. *Planes conjuntos de auditoría.*

1. La Autoridad Vasca de Protección de Datos podrá desarrollar acciones comunes de auditoría con las restantes autoridades de protección de datos del Estado.

2. Dentro de dichas actividades, podrán llevarse a cabo actuaciones de investigación conjuntas con participación del personal de las distintas autoridades. En estos supuestos, el personal de la Autoridad Vasca de Protección de Datos competente para realizar las actuaciones de inspección, conforme a la sección 3.ª del capítulo II de esta ley, coordinará la actividad de los restantes intervinientes cuando se tratase de responsables o encargados del tratamiento sometidos a esta ley, actuando dichos intervinientes bajo la dirección y coordinación del personal de la Autoridad Vasca de Protección de Datos.

3. La Autoridad Vasca de Protección de Datos podrá dictar, respecto de los sujetos sometidos a esta ley, las directrices que procedan como consecuencia de la realización de los planes de auditoría, sin perjuicio de las que se adoptasen conjuntamente por todas las autoridades intervinientes.

Artículo 23. *Cooperación en el marco de los procedimientos transfronterizos.*

1. La Autoridad Vasca de Protección de Datos podrá tener la consideración de autoridad principal o interesada en los procedimientos transfronterizos, de acuerdo con lo establecido en los artículos 56 y 60 del Reglamento (UE) 2016/679.

2. Cuando la Autoridad Vasca de Protección de Datos intervenga en un procedimiento coordinado relacionado con un tratamiento transfronterizo de datos personales o alguna de sus decisiones haya de someterse a aprobación del Comité Europeo de Protección de Datos, intervendrá en las reuniones de dicho comité en los términos establecidos en los artículos 60 a 62 de la Ley Orgánica 3/2018, de 5 de diciembre.

3. La asistencia y cooperación entre autoridades de protección de datos de los estados miembros de la Unión Europea, en el marco de la Ley Orgánica 7/2021 de 26 de mayo, se someterá a lo dispuesto en su artículo 51.

CAPÍTULO III

Régimen sancionador. Potestad correctiva de la Autoridad Vasca de Protección de Datos

Artículo 24. *Sujetos responsables.*

1. Los responsables y encargados de los tratamientos a los que se refiere el artículo 2 de esta ley están sujetos al régimen de infracciones y sanciones contenido en este capítulo.

2. Asimismo, el régimen sancionador de esta ley será aplicable a:

a) Las entidades acreditadas de supervisión de los códigos de conducta aprobados por la Autoridad Vasca de Protección de Datos, conforme a lo dispuesto en el artículo 18.

b) Las entidades de certificación acreditadas por la Autoridad Vasca de Protección de Datos conforme a lo dispuesto en el artículo 19.

Artículo 25. *Infracciones.*

1. Constituyen infracciones de la presente ley los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, y los artículos 72 a 74 de la Ley Orgánica 3/2018, de 5 de diciembre.

2. Asimismo, constituyen infracciones de la presente ley los actos y conductas a las que se refieren los artículos 58 a 60 de la Ley Orgánica 7/2021, de 26 de mayo.

3. La Autoridad Vasca de Protección de Datos será competente para sancionar las infracciones cometidas por los sujetos responsables a los que se refiere el artículo anterior, a excepción de las conductas tipificadas en los artículos 58.j) y 59.j) de la Ley Orgánica 7/2021, de 26 de mayo.

Artículo 26. *Prescripción de las infracciones.*

1. Las infracciones a que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 prescribirán a los tres años, a los dos años o al año, según se califiquen como muy graves, graves o leves, de acuerdo con los artículos 72 a 74 de la Ley Orgánica 3/2018, de 5 de diciembre.

2. Las infracciones tipificadas en la Ley Orgánica 7/2021, de 26 de mayo, prescribirán a los seis meses, a los dos años o a los tres años de haberse cometido, según sean leves, graves o muy graves, respectivamente.

3. Interrumpirá la prescripción de la infracción la iniciación, con conocimiento de la persona interesada, del procedimiento establecido en el capítulo IV de esta ley, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables a la presunta persona infractora.

Artículo 27. *Sanciones administrativas y medidas correctivas.*

1. El régimen contenido en el presente artículo será de aplicación a:

a) Los entes de naturaleza jurídica privada pertenecientes al sector público vasco.

b) Las personas físicas y las entidades privadas que presten servicios públicos mediante cualquier forma de gestión directa o indirecta o que ostenten la condición de encargados del tratamiento sometidos a esta ley conforme a su artículo 2.2.

c) Las entidades acreditadas de supervisión de los códigos de conducta y las entidades de certificación acreditadas por la Autoridad Vasca de Protección de Datos cuando tengan naturaleza jurídica privada.

2. Las infracciones a que se refiere el artículo 25 de esta ley serán sancionadas con multa en los términos recogidos en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, y en el artículo 62.2 de la Ley Orgánica 7/2021, de 26 de mayo.

Para la determinación de su importe se atenderá a los criterios establecidos en los artículos 83.2 del Reglamento (UE) 2016/679 y 76.2 de la Ley Orgánica 3/2018, de 5 de diciembre.

3. Las multas se impondrán en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas establecidas en el artículo 58.2, letras a) a h) y j) del Reglamento (UE) 2016/679.

Artículo 28. *Régimen aplicable a las administraciones, entidades e instituciones públicas vascas.*

1. Cuando las administraciones, entidades e instituciones públicas vascas incluidas en el ámbito de aplicación de esta ley, actuando como responsables o encargados del tratamiento, cometiesen alguna de las infracciones contempladas en ella, la Autoridad Vasca de Protección de Datos dictará resolución declarando la infracción y dirigiendo un apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

2. La resolución adoptada se notificará al responsable o encargado del tratamiento, así como, en su caso, al órgano del que dependa jerárquicamente, y a la persona denunciante.

3. La persona denunciante que no ostente la condición de interesada no tendrá más participación en el procedimiento que el derecho a conocer sobre la apertura o no del procedimiento y, en su caso, de la resolución que le ponga fin.

4. Sin perjuicio de lo establecido en el apartado anterior, la Autoridad Vasca de Protección de Datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

5. Asimismo, cuando las infracciones sean imputables a autoridades, altos cargos y personal directivo, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con la denominación del cargo que fuese responsable y se ordenará su publicación en el «Boletín Oficial del País Vasco».

6. Si la autoridad, alto cargo o personal directivo estuviese sometido al Código Ético y de Conducta de los cargos públicos y personal eventual de la Administración General e Institucional de la Comunidad Autónoma del País Vasco, se dará igualmente traslado de la resolución a la Comisión de Ética Pública, a fin de que le dé el trámite que proceda y, particularmente, garantice el cumplimiento del principio de responsabilidad establecido en el citado código ético.

7. Se deberán comunicar a la Autoridad Vasca de Protección de Datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los dos apartados anteriores.

8. Se comunicarán al Ararteko las resoluciones sancionadoras dictadas al amparo de este artículo.

Artículo 29. *Publicidad de las sanciones.*

Sin perjuicio de las obligaciones de transparencia establecidas en el artículo 7 de esta ley, la Autoridad Vasca de Protección de Datos hará públicas en el «Boletín Oficial del País Vasco»:

a) La información que identifique a la persona infractora, la infracción cometida y el importe de la sanción impuesta cuando exceda de un millón de euros y la persona infractora sea una persona jurídica.

b) Las amonestaciones a las que se refiere el párrafo segundo del artículo 28.5 de esta ley.

Artículo 30. *Prescripción de las sanciones.*

1. Las sanciones económicas impuestas en aplicación del Reglamento (UE) 2016/679 y de esta ley prescriben en los siguientes plazos:

a) Las sanciones por importe igual o inferior a 40.000 euros prescriben en el plazo de un año.

b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.

c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. Las sanciones económicas impuestas en aplicación de la Ley Orgánica 7/2021, de 26 de mayo, prescriben en los siguientes plazos:

a) Las sanciones por importe comprendido entre 6.000 y 60.000 euros prescriben en el plazo de un año.

b) Las sanciones por importe comprendido entre 60.001 y 360.000 euros prescriben en el plazo de dos años.

c) Las sanciones por importe comprendido entre 360.001 y 1.000.000 de euros prescriben en el plazo de tres años.

3. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

4. La prescripción se interrumpirá por la iniciación, con conocimiento de la persona interesada, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable a la persona infractora.

CAPÍTULO IV

Procedimientos en caso de infracción de las normas de protección de datos

Sección 1.ª Disposiciones generales

Artículo 31. *Régimen jurídico.*

1. Las disposiciones de este capítulo serán de aplicación a los siguientes procedimientos tramitados por la Autoridad Vasca de Protección de Datos:

a) Aquellos en los que una persona afectada reclame que no ha sido adecuadamente atendida su solicitud de ejercicio de los derechos consagrados por los artículos 15 a 22 del Reglamento (UE) 2016/679 y 21 a 23 de la Ley Orgánica 7/2021, de 26 de mayo.

b) Aquellos que tienen por objeto la determinación de la posible existencia de una infracción en materia de protección de datos.

c) Aquellos procedimientos transfronterizos en los que la Autoridad Vasca de Protección de Datos tenga la condición de autoridad principal conforme a lo dispuesto en el Reglamento (UE) 2016/679.

2. Dichos procedimientos se regirán, en lo que resulte aplicable, por el Reglamento (UE) 2016/679, así como por lo dispuesto en el presente capítulo y las disposiciones de desarrollo de esta ley.

3. Será de aplicación subsidiaria a los procedimientos sancionadores lo establecido en la normativa reguladora del ejercicio de la potestad sancionadora de las administraciones públicas de la Comunidad Autónoma del País Vasco.

Artículo 32. *Causas de suspensión del procedimiento.*

1. Los plazos de tramitación establecidos en este capítulo, así como los de admisión a trámite regulados por el artículo 34.4 y de duración de las actuaciones previas de investigación previstos en el artículo 38.2, quedarán automáticamente suspendidos cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de un órgano u organismo de la Unión Europea o de una o varias autoridades de control de otros estados miembros conforme con lo establecido en el Reglamento (UE) 2016/679, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Autoridad Vasca de Protección de Datos. Esta suspensión se comunicará a la persona interesada.

2. Los plazos de tramitación quedarán igualmente suspendidos en los supuestos establecidos en la legislación básica y autonómica reguladora del procedimiento administrativo.

3. En particular, los plazos quedarán suspendidos en los supuestos en que proceda la determinación de la autoridad de control principal en caso de procedimientos relacionados con tratamientos transfronterizos, así como la tramitación del procedimiento coordinado establecido en los artículos 60 y 63 del Reglamento (UE) 2016/679.

4. El transcurso de los plazos de tramitación se podrá suspender, mediante resolución motivada, cuando resulte indispensable recabar información de un órgano jurisdiccional.

Sección 2.ª Iniciación del procedimiento

Artículo 33. *Tramitación en caso de reclamación. Actuaciones previas a la admisión a trámite.*

1. En todos los supuestos en que se formule ante la Autoridad Vasca de Protección de Datos una reclamación en los términos establecidos en el artículo 57.1.f) del Reglamento (UE) 2016/679, o en el artículo 52 de la Ley Orgánica 7/2021, de 26 de mayo, aquella procederá, con carácter previo a la realización de cualquier otra actuación, a examinar su competencia y determinar si el tratamiento al que la reclamación se refiere tiene carácter transfronterizo, conforme a lo dispuesto en el citado reglamento.

2. La Autoridad Vasca de Protección de Datos dará inmediatamente traslado de la reclamación a quien resulte competente cuando aprecie que la competencia corresponde a otra autoridad de protección de datos del Estado o, en caso de tratarse de un procedimiento trasfronterizo, a la autoridad de control de otro Estado miembro de la Unión Europea que ostente la condición de autoridad principal conforme al Reglamento (UE) 2016/679. El traslado de la reclamación y su archivo provisional se notificarán a la persona reclamante.

3. Verificada la competencia de la Autoridad Vasca de Protección de Datos, esta podrá dar traslado de la reclamación al responsable o encargado del tratamiento contra el que se dirija dicha reclamación, a fin de que, en el plazo máximo de un mes, realice las aclaraciones y alegaciones que estime necesarias en relación con la reclamación presentada. Cuando el responsable o encargado hubiese notificado a la Autoridad Vasca de Protección de Datos la

designación de un delegado o delegada de protección de datos, el traslado de la reclamación se realizará a través de este.

Si transcurrido el plazo de un mes no se hubiera comunicado a la Autoridad Vasca de Protección de Datos la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento.

4. Igualmente, si el responsable o encargado del tratamiento se encontrasen adheridos a un código de conducta, la Autoridad Vasca de Protección de Datos podrá dar traslado de la reclamación a su órgano de supervisión, a fin de que informe lo que proceda en el plazo de un mes.

Artículo 34. *Admisión a trámite de las reclamaciones.*

1. La Autoridad Vasca de Protección de Datos notificará, dentro de los tres meses siguientes a la fecha de recepción de la reclamación, la resolución por la que acordará su admisión o inadmisión a trámite.

2. En el acuerdo de admisión a trámite la Autoridad Vasca de Protección de Datos especificará el tipo de procedimiento que origina la reclamación formulada.

3. Cuando se hubiese presentado ante la Autoridad Vasca de Protección de Datos una reclamación referida a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, o 21 a 23 de la Ley Orgánica 7/2021, de 26 de mayo, o a la existencia de hechos que pudiesen ser constitutivos de una infracción de la normativa de protección de datos, la Autoridad Vasca de Protección de Datos podrá acordar la admisión a trámite de dos procedimientos diferenciados, que se tramitarán, respectivamente, conforme a lo establecido en las secciones 3.ª y 4.ª de este capítulo.

4. Transcurridos tres meses desde la recepción de la reclamación sin que se hubiera notificado a la persona reclamante la decisión sobre su admisión a trámite, se entenderá admitida la reclamación desde esa fecha y proseguirá su tramitación conforme a los procedimientos establecidos en las secciones 3.ª y 4.ª de este capítulo.

Artículo 35. *Inadmisión a trámite.*

1. La Autoridad Vasca de Protección de Datos acordará la inadmisión a trámite de la reclamación en caso de que la misma no verse sobre cuestiones de protección de datos personales, carezca notoriamente de fundamento, sea abusiva o no aporte indicios racionales de la existencia de una infracción.

2. Igualmente, la Autoridad Vasca de Protección de Datos podrá inadmitir a trámite la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por aquella, hubiera adoptado medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio a la persona afectada en el caso de las infracciones con la consideración de leves a efectos de prescripción.

b) Que el derecho de la persona afectada quede plenamente garantizado mediante la aplicación de las medidas adoptadas.

Artículo 36. *Otros supuestos de iniciación del procedimiento.*

La Autoridad Vasca de Protección de Datos podrá igualmente acordar el inicio del procedimiento en los siguientes supuestos:

a) Cuando le fuera comunicada por una autoridad de control perteneciente a otro Estado miembro de la Unión Europea una reclamación formulada ante ella, y la Autoridad Vasca de Protección de Datos ostentase la condición de autoridad de control principal para la tramitación de un procedimiento conforme a lo dispuesto en los artículos 56 y 60 del Reglamento (UE) 2016/679.

b) Cuando le sea remitida por otra autoridad de protección de datos del Estado la reclamación que se hubiese formulado ante aquella y fuera la Autoridad Vasca de Protección de Datos la competente para conocer de la reclamación conforme al artículo 2 de esta ley.

c) Cuando así lo determinase la Autoridad Vasca de Protección de Datos al tener conocimiento de la existencia de indicios de la comisión de una infracción de lo dispuesto en la normativa de protección de datos personales.

Sección 3.ª Procedimiento en caso de reclamaciones derivadas del ejercicio de derechos

Artículo 37. *Tramitación del procedimiento.*

1. Admitida a trámite la reclamación o transcurrido el plazo para ello, la Autoridad Vasca de Protección de Datos la remitirá al responsable del tratamiento a fin de que este, en el plazo de quince días, formule las alegaciones que estime pertinentes.

2. Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Autoridad Vasca de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia de la persona afectada y nuevamente del responsable del tratamiento, resolverá sobre la reclamación formulada.

3. El plazo máximo para resolver el procedimiento será de seis meses a contar desde la notificación a la persona reclamante del acuerdo de admisión a trámite, o desde el transcurso del plazo de tres meses sin que se notifique a la persona reclamante la decisión sobre la admisión de su reclamación.

4. Transcurrido el plazo máximo de seis meses para resolver, la persona afectada podrá considerar desestimada su reclamación.

Sección 4.ª Procedimiento de ejercicio de la potestad sancionadora

Artículo 38. *Actuaciones previas de investigación.*

1. Antes de la adopción del acuerdo de inicio del procedimiento sancionador, la Autoridad Vasca de Protección de Datos podrá acordar la realización de las actuaciones previas de investigación que resulten necesarias a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento de ejercicio de la potestad sancionadora.

La Autoridad Vasca de Protección de Datos podrá acordar la realización de las actuaciones previas de investigación a través de sistemas digitales en los términos previstos en el artículo 53 bis de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, con una duración máxima de 18 meses.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en la sección 3.ª del capítulo II de esta ley y no podrán tener una duración superior a los 18 meses a contar desde la fecha del acuerdo de admisión a trámite o desde que se hubiera cumplido el plazo para adoptarlo, o desde que la propia Autoridad decida su iniciación en los supuestos a los que se refiere el artículo 36 de esta ley.

Artículo 39. *Procedimiento sancionador.*

1. Concluidas, en su caso, las actuaciones de investigación, la presidencia de la Autoridad Vasca de Protección de Datos dictará, cuando así proceda, acuerdo de iniciación del procedimiento sancionador.

2. El plazo máximo para dictar resolución será de 12 meses a contar desde la fecha del acuerdo de inicio. Transcurrido este plazo sin que dicte resolución se producirá la caducidad del procedimiento.

3. En lo demás, el procedimiento se regulará por lo establecido en la normativa reguladora del ejercicio de la potestad sancionadora de las administraciones públicas de la Comunidad Autónoma del País Vasco, sin perjuicio de la aplicación, en su caso, de lo establecido en la sección 5.ª de este capítulo.

4. Cuando así proceda, en atención a la naturaleza de los hechos y teniendo debidamente en cuenta los criterios establecidos en el artículo 83.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Autoridad Vasca de Protección de Datos, previa audiencia al responsable o encargado del tratamiento, podrá dirigir un apercibimiento, así como ordenar al responsable o encargado del tratamiento que

adopte las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos de una determinada manera y dentro del plazo especificado. El procedimiento tendrá una duración máxima de seis meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

Artículo 40. *Medidas cautelares.*

1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la presidencia de la Autoridad Vasca de Protección de Datos podrá acordar motivadamente las medidas provisionales o cautelares necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.

2. Igualmente podrá acordar la adopción de las medidas cautelares establecidas en la normativa reguladora del ejercicio de la potestad sancionadora de las administraciones públicas de la Comunidad Autónoma del País Vasco.

3. En los casos en que la Autoridad Vasca de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportará un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

4. Será igualmente posible la adopción excepcional de medidas cautelares por los inspectores o inspectoras de la Autoridad Vasca de Protección de Datos que estuviesen llevando a cabo las actuaciones previas de investigación en los supuestos y con las condiciones establecidas en la normativa reguladora del ejercicio de la potestad sancionadora de las administraciones públicas de la Comunidad Autónoma del País Vasco.

Sección 5.ª Especialidades en caso de procedimientos referidos a tratamientos transfronterizos

Artículo 41. *Especialidades aplicables a los procedimientos transfronterizos en que la Autoridad Vasca de Protección de Datos sea autoridad principal.*

Cuando la Autoridad Vasca de Protección de Datos tuviera la condición de autoridad principal en un procedimiento de los regulados por el artículo 60 del Reglamento (UE) 2016/679, una vez realizados los trámites y actuaciones complementarias que resulten necesarias para la adecuada ordenación del procedimiento, aquella dictará proyecto de resolución del que se dará traslado a las restantes autoridades interesadas a los efectos previstos en el artículo 60.3 del citado reglamento.

Será en este supuesto de aplicación lo dispuesto en el artículo 60 y, en su caso, en el artículo 63 del Reglamento (UE) 2016/679.

Artículo 42. *Especialidades aplicables a los procedimientos transfronterizos en los que la Autoridad Vasca de Protección de Datos sea autoridad interesada ante la que se hubiese formulado reclamación por una persona afectada.*

1. Cuando la Autoridad Vasca de Protección de Datos tuviera la condición de autoridad interesada en un procedimiento de los regulados por el artículo 60 del Reglamento (UE) 2016/679, dará inmediatamente traslado de la reclamación formulada ante ella a la autoridad principal, a fin de que proceda a la tramitación del procedimiento conforme a lo dispuesto en el artículo 60 del citado reglamento.

2. El acuerdo por el que se resuelva la remisión a la que se refiere el párrafo anterior implicará el archivo provisional del procedimiento, sin perjuicio de que por la Autoridad Vasca de Protección de Datos se dicte, en caso de que así proceda, la resolución a la que se refieren los apartados 8 y 9 del artículo 60 del Reglamento (UE) 2016/679.

Disposición adicional primera. *Normativa aplicable a los procedimientos tramitados por la Autoridad Vasca de Protección de Datos no regulados por esta ley.*

La legislación básica y autonómica reguladora del procedimiento administrativo será de aplicación a los procedimientos cuya tramitación corresponda a la Autoridad Vasca de Protección de Datos, en virtud de lo establecido en esta u otras leyes y que no se encuentren expresamente regulados por el capítulo IV de esta ley.

Disposición adicional segunda. *Agencia Vasca de Protección de Datos.*

1. La Autoridad Vasca de Protección de Datos se subroga en la posición jurídica de la Agencia Vasca de Protección de Datos en cuanto a los bienes, derechos y obligaciones de que fuera titular la Agencia.

2. Las referencias hechas en el ordenamiento jurídico a la Agencia Vasca de Protección de Datos deben entenderse hechas a la Autoridad Vasca de Protección de Datos.

Disposición adicional tercera. *Creación de cuerpos y escalas de personal funcionario propio de la Autoridad Vasca de Protección de Datos.*

1. El personal funcionario propio de la Autoridad Vasca de Protección de Datos se agrupa en cuerpos y escalas, según el nivel de titulación exigido para el acceso a dichos cuerpos y escalas, conforme a lo previsto en el artículo 76 del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público, y según lo previsto en el artículo 15 de la Ley 7/2021, de 11 de noviembre, de los cuerpos y de las escalas de la Administración de la Comunidad Autónoma de Euskadi.

2. Se crean los siguientes cuerpos y escalas, en los cuales se integrará el personal funcionario propio de la Autoridad:

Cuerpo Superior (Subgrupo de clasificación A1).

– Escala Superior de Administración de la Autoridad Vasca de Protección de Datos.

– Escala Superior Facultativa Jurídica de la Autoridad Vasca de Protección de Datos.

– Escala Superior Facultativa de Sistemas de Información de la Autoridad Vasca de Protección de Datos.

– Escala Superior Facultativa de Archivo, Biblioteca y Documentación de la Autoridad Vasca de Protección de Datos.

– Escala Superior Facultativa de Traducción de la Autoridad Vasca de Protección de Datos.

Cuerpo Técnico (Grupo de clasificación B).

– Escala Técnica de Informática de Gestión de la Autoridad Vasca de Protección de Datos.

Cuerpo Administrativo (Subgrupo de clasificación C1).

– Escala Administrativa de la Autoridad Vasca de Protección de Datos.

Cuerpo Auxiliar Administrativo (Subgrupo de clasificación C2).

– Escala Auxiliar Administrativa de la Autoridad Vasca de Protección de Datos.

3. De acuerdo con lo establecido en el artículo 5 de la presente ley, la relación de puestos de trabajo de la entidad establecerá la adscripción de cada puesto de trabajo a los cuerpos y escalas establecidos en la presente disposición adicional.

4. El acceso del personal funcionario propio se producirá al cuerpo y escala correspondiente al que esté adscrita la plaza objeto de la convocatoria. La provisión de puestos de trabajo por personal procedente de otras administraciones públicas se realizará de acuerdo con lo establecido, en su caso, en la relación de puestos de trabajo.

5. Por resolución de la presidencia de la Autoridad se podrá incluir, asimismo, un sistema de equivalencias entre los cuerpos y escalas propios y de los puestos de trabajo de la Autoridad, y los cuerpos, escalas, clases y categorías de otras administraciones públicas.

Disposición transitoria primera. *Régimen de la Autoridad Vasca de Protección de Datos.*

1. El Estatuto de la Agencia Vasca de Protección de Datos, aprobado por el Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos, será aplicable a la Autoridad Vasca de Protección de Datos en cuanto no se oponga a lo dispuesto en la presente ley, mientras no se adopte el estatuto de esta última.

2. Lo dispuesto en el apartado 5 del artículo 8 y en el apartado 1 del artículo 9 será de aplicación una vez expire el mandato de la persona que ostente la dirección de la Agencia Vasca de Protección de Datos y de quienes conformen su consejo consultivo en el momento de entrada en vigor de esta ley.

Disposición transitoria segunda. *Régimen transitorio de los procedimientos.*

Las actuaciones previas de investigación y los procedimientos administrativos iniciados con anterioridad a la entrada en vigor de esta ley continuarán tramitándose de conformidad con la normativa aplicable en el momento de su inicio.

Disposición transitoria tercera. *Integración del personal funcionario de la Agencia Vasca de Protección de Datos en los cuerpos y escalas del personal funcionario de la Autoridad Vasca de Protección de Datos.*

1. El personal con nombramiento de funcionaria o funcionario de carrera de la Agencia Vasca de Protección de Datos a la entrada en vigor de esta ley, como consecuencia de los procesos de estabilización excepcional convocados previamente, se integrará en los cuerpos y escalas correspondientes de la Autoridad Vasca de Protección de Datos a los que se adscriban las plazas que ocupen en la relación de puestos de trabajo.

2. Las funcionarias y funcionarios de carrera integrados en cuerpos y escalas de otras administraciones públicas que desempeñen, como titulares, puestos de trabajo de la Agencia Vasca de Protección de Datos a la entrada en vigor de esta ley, podrán optar por integrarse en los cuerpos y escalas correspondientes de la Autoridad Vasca de Protección de Datos, en los términos que reglamentariamente se determine.

3. El personal funcionario que ocupe puestos de trabajo de la Agencia Vasca de Protección de Datos en régimen de comisión de servicios o como personal funcionario interino continuará en las mismas condiciones en que viniera prestando sus servicios.

Disposición derogatoria.

Quedan derogadas las siguientes disposiciones normativas:

– Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

– Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

– Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos.

Disposición final. *Entrada en vigor.*

La presente ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del País Vasco».

§ 31

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 298, de 12 de noviembre de 2020
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2020-14046

[. . .]

TÍTULO III

Obligaciones y responsabilidad de los prestadores de servicios electrónicos de confianza

Artículo 8. *Protección de los datos personales.*

1. El tratamiento de los datos personales que precisen los prestadores de servicios electrónicos de confianza para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta Ley se sujetará a lo dispuesto en la legislación aplicable en materia de protección de datos de carácter personal.

2. Los prestadores de servicios electrónicos de confianza que consignen un pseudónimo en un certificado electrónico deberán constatar la verdadera identidad del titular del certificado y conservar la documentación que la acredite.

3. Dichos prestadores de servicios de confianza estarán obligados a revelar la citada identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas en el ejercicio de funciones legalmente atribuidas, con sujeción a lo dispuesto en la legislación aplicable en materia de protección de datos personales.

Artículo 9. *Obligaciones de los prestadores de servicios electrónicos de confianza.*

1. Los prestadores de servicios electrónicos de confianza deberán:

a) Publicar información veraz y acorde con esta Ley y el Reglamento (UE) 910/2014.

b) No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.

En este caso, utilizarán sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, y se aplicarán procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado. Además, deberán custodiar y proteger los datos de creación de firma, sello o autenticación de sitio web frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

2. Los prestadores de servicios de confianza que expidan certificados electrónicos deberán disponer de un servicio de consulta sobre el estado de validez o revocación de los certificados emitidos accesible al público.

3. Los prestadores cualificados de servicios electrónicos de confianza deberán cumplir las siguientes obligaciones adicionales:

a) El período de tiempo durante el que deberán conservar la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014, será de 15 años desde la extinción del certificado o la finalización del servicio prestado.

En caso de que expidan certificados cualificados de sello electrónico o autenticación de sitio web a personas jurídicas, los prestadores de servicios de confianza registrarán también la información que permita determinar la identidad de la persona física a la que se hayan entregado los citados certificados, para su identificación en procedimientos judiciales o administrativos.

b) Constituir un seguro de responsabilidad civil por importe mínimo de 1.500.000 euros, excepto si el prestador pertenece al sector público. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, se añadirán 500.000 euros más por cada tipo de servicio.

La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea coherente con lo dispuesto en el párrafo anterior.

Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto.

c) El prestador cualificado que vaya a cesar en su actividad deberá comunicarlo a los clientes a los que preste sus servicios y al órgano de supervisión con una antelación mínima de dos meses al cese efectivo de la actividad, por un medio que acredite la entrega y recepción efectiva siempre que sea factible. El plan de cese del prestador de servicios puede incluir la transferencia de clientes, una vez acreditada la ausencia de oposición de los mismos, a otro prestador cualificado, el cual podrá conservar la información relativa a los servicios prestados hasta entonces.

Igualmente, comunicará al órgano de supervisión cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.

d) Enviar el informe de evaluación de la conformidad al Ministerio de Asuntos Económicos y Transformación Digital en los términos previstos en el artículo 20.1 del Reglamento (UE) 910/2014. El incumplimiento de esta obligación conllevará la retirada de la cualificación al prestador y al servicio que este presta, y su eliminación de la lista de confianza prevista en el artículo 22 del citado Reglamento, previo requerimiento al prestador del servicio para que cese en el citado incumplimiento.

Artículo 10. *Responsabilidad de los prestadores de servicios electrónicos de confianza.*

Los prestadores de servicios electrónicos de confianza asumirán toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios electrónicos de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

Artículo 11. *Limitaciones de responsabilidad de los prestadores de servicios electrónicos de confianza.*

1. El prestador de servicios electrónicos de confianza no será responsable de los daños y perjuicios ocasionados a la persona a la que ha prestado sus servicios o a terceros de buena fe, si esta incurre en alguno de los supuestos previstos en el Reglamento (UE) 910/2014 o en los siguientes:

a) No haber proporcionado al prestador de servicios de confianza información veraz, completa y exacta para la prestación del servicio de confianza, en particular, sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o

para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada, actuando con la debida diligencia, por el prestador de servicios.

b) La falta de comunicación sin demora indebida al prestador de servicios de cualquier modificación de las circunstancias que incidan en la prestación del servicio de confianza, en particular, aquellas reflejadas en el certificado electrónico.

c) Negligencia en la conservación de sus datos de creación de firma, sello o autenticación de sitio web, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de estos o, en su caso, de los medios que den acceso a ellos.

d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma, sello o autenticación de sitio web o, en su caso, de los medios que den acceso a ellos.

e) Utilizar los datos de creación de firma, sello o autenticación de sitio web cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de confianza le notifique la extinción o suspensión de su vigencia.

2. El prestador de servicios de confianza tampoco será responsable por los daños y perjuicios si el destinatario actúa de forma negligente. Se entenderá que el destinatario actúa de forma negligente cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico, o cuando no verifique la firma o sello electrónico.

3. El prestador de servicios de confianza no será responsable por los daños y perjuicios en caso de inexactitud de los datos que consten en el certificado electrónico si estos le han sido acreditados mediante documento público u oficial, inscrito en un registro público si así resulta exigible.

Artículo 12. *Inicio de la prestación de servicios electrónicos de confianza no cualificados.*

Los prestadores de servicios de confianza no cualificados no necesitan verificación administrativa previa de cumplimiento de requisitos para iniciar su actividad, pero deberán comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el plazo de tres meses desde que la inicien, que publicará en su página web el listado de prestadores de servicios de confianza no cualificados en una lista diferente a la de los prestadores de servicios de confianza cualificados, con la descripción detallada y clara de las características propias y diferenciales de los prestadores cualificados y de los prestadores no cualificados.

En el mismo plazo deberán comunicar la modificación de los datos inicialmente transmitidos y el cese de su actividad.

Artículo 13. *Obligaciones de seguridad de la información.*

1. Los prestadores cualificados y no cualificados de servicios electrónicos de confianza notificarán al Ministerio de Asuntos Económicos y Transformación Digital las violaciones de seguridad o pérdidas de la integridad señaladas en el artículo 19.2 del Reglamento (UE) 910/2014, sin perjuicio de su notificación a la Agencia Española de Protección de Datos, a otros organismos relevantes o a las personas afectadas.

2. Los prestadores de servicios tienen la obligación de tomar las medidas necesarias para resolver los incidentes de seguridad que les afecten.

3. Los prestadores de servicios ampliarán, en un plazo máximo de un mes tras la notificación del incidente y, de haber tenido lugar, tras su resolución, la información suministrada en la notificación inicial con arreglo a las directrices y formularios que pueda establecer el Ministerio de Asuntos Económicos y Transformación Digital.

[. . .]

§ 32

Real Decreto-ley 26/2020, de 7 de julio, de medidas de reactivación económica para hacer frente al impacto del COVID-19 en los ámbitos de transportes y vivienda. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 187, de 8 de julio de 2020
Última modificación: 2 de agosto de 2022
Referencia: BOE-A-2020-7432

[. . .]

CAPÍTULO II

Medidas en el sector del transporte aéreo

Artículo 2. *Medidas de gestión de pasajeros aéreos y del personal de aviación en relación a la pandemia COVID-19.*

(Derogado)

Artículo 3. *Directrices operativas para la gestión de pasajeros aéreos y personal de aviación en relación a la pandemia COVID-19.*

(Derogado)

Artículo 4. *Obligaciones de los gestores aeroportuarios y de las compañías aéreas.*

(Derogado)

Artículo 5. *Obligaciones de los pasajeros.*

(Derogado)

Artículo 6. *Limitación de acceso a los edificios terminales de los aeropuertos.*

(Derogado)

Artículo 7. *Órganos de coordinación, aplicación y supervisión en la aplicación y supervisión de las Directrices EASA/ECDC.*

(Derogado)

[. . .]

Disposición adicional primera. *Protección de datos de carácter personal.*

1. El tratamiento de la información de carácter personal que se realice como consecuencia del desarrollo y aplicación del capítulo II, se hará de acuerdo a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, cuando proceda, en lo establecido en los artículos ocho.1 y veintitrés de la Ley 14/1986, de 25 de abril, General de Sanidad. En particular, las obligaciones de información a los interesados relativas a los datos obtenidos por los sujetos incluidos en el ámbito de aplicación de este capítulo se ajustarán a lo dispuesto en el artículo 14 del Reglamento general de protección de datos, teniendo en cuenta las excepciones y obligaciones previstas en su apartado 5.

2. El tratamiento tendrá por finalidad el seguimiento y vigilancia epidemiológica del COVID-19 para prevenir y evitar situaciones excepcionales de especial gravedad, atendiendo a razones de interés público esencial en el ámbito específico de la salud pública, y para la protección de intereses vitales de los afectados y de otras personas físicas al amparo de lo establecido en el Reglamento general de protección de datos. Los datos recabados serán utilizados exclusivamente con esta finalidad.

En la obtención y tratamiento de estos datos no será necesaria la obtención del consentimiento del pasajero, en virtud de lo dispuesto en el artículo 6.1, letra e), del Reglamento general de protección de datos.

3. Los gestores aeroportuarios y compañías aéreas que colaboren con las autoridades competentes del Ministerio de Sanidad, en la implementación de los controles sanitarios, no podrán almacenar, acceder o tratar los datos de salud y cualquier otro conexo obtenidos en el ejercicio de dicha colaboración.

4. El intercambio de datos con otros países se regirá por el Reglamento general de protección de datos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, teniendo en cuenta la Decisión n.º 1082/2013/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud y por la que se deroga la Decisión n ° 2119/98/CE.

[. . .]

Información relacionada

- Véase, en cuanto a la extensión del plazo de solicitud y de duración de moratorias y suspensiones concedidas al amparo de la presente disposición, los arts. 7 y 8 del Real Decreto-ley 3/2021, de 2 de febrero, por el que se adoptan medidas para la reducción de la brecha de género y otras materias en los ámbitos de la Seguridad Social y económico. Ref. BOE-A-2021-1529
- El Real Decreto-ley 26/2020, de 7 de julio ha sido convalidado por Acuerdo del Congreso de los Diputados, publicado por Resolución de 22 de julio de 2020. Ref. BOE-A-2020-8634

§ 33

Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 284, de 24 de noviembre de 2018
Última modificación: 28 de diciembre de 2023
Referencia: BOE-A-2018-16036

[. . .]

TÍTULO III

Derechos y obligaciones en relación con la prestación y utilización de servicios de pago

[. . .]

CAPÍTULO II

Autorización de operaciones de pago

[. . .]

Artículo 37. *Confirmación de la disponibilidad de fondos.*

1. Los proveedores de servicios de pago gestores de cuenta, previa solicitud de un proveedor de servicios de pago que emita instrumentos de pago basados en tarjetas, confirmarán inmediatamente la disponibilidad de fondos en la cuenta de pago del ordenante para la ejecución de una operación de pago basada en una tarjeta, siempre que se cumplan todas las condiciones siguientes:

a) que la cuenta de pago del ordenante sea accesible en línea en el momento de la solicitud;
b) que el ordenante haya dado consentimiento explícito al proveedor de servicios de pago gestor de cuenta para que responda a las solicitudes de proveedores de servicios de pago específicos de facilitar confirmación de que el importe correspondiente a una operación de pago basada en una tarjeta determinada está disponible en la cuenta de pago del ordenante;
c) que el consentimiento a que hace referencia la letra b) debe darse antes de que se realice la primera solicitud de confirmación.

2. El proveedor de servicios de pago podrá solicitar la confirmación a que hace referencia el apartado 1 cuando se cumplan todas las condiciones siguientes:

a) que el ordenante haya dado consentimiento explícito al proveedor de servicios de pago que solicite dicha confirmación;

b) que el ordenante haya iniciado la operación de pago basada en una tarjeta por el importe en cuestión utilizando un instrumento de pago basado en tarjeta emitido por el proveedor de servicios de pago;

c) que el proveedor de servicios de pago se identifique ante el proveedor de servicios de pago gestor de cuenta antes de cada solicitud de confirmación, y se comunique de manera segura con el proveedor de servicios de pago gestor de cuenta, de conformidad con lo previsto en el Reglamento Delegado 2018/389 y a los criterios que, dentro de las disposiciones de la Autoridad Bancaria Europea que le resulten aplicables, determine el Banco de España.

3. De conformidad con la normativa de protección de datos personales, la confirmación a que hace referencia el apartado 1 consistirá únicamente en una simple respuesta de «sí» o «no» y no en un extracto del saldo de cuenta. Esa respuesta no se conservará ni utilizará para fines distintos de la ejecución de la operación de pago con tarjeta.

4. La confirmación a que hace referencia el apartado 1 no permitirá al proveedor de servicios de pago gestor de cuenta bloquear fondos en la cuenta de pago del ordenante.

5. El ordenante podrá solicitar al proveedor de servicios de pago gestor de cuenta que le comunique la identificación del proveedor de servicios de pago y la respuesta facilitada.

6. El presente artículo no se aplicará a las operaciones de pago iniciadas mediante instrumentos de pago basados en tarjetas en los que se almacene dinero electrónico tal como se define en la Ley 21/2011, de 26 de julio, de dinero electrónico.

[. . .]

Artículo 39. *Normas de acceso a la información sobre cuentas de pago y uso de dicha información en caso de servicios de información sobre cuentas.*

1. El proveedor de servicios de pago que preste el servicio de información sobre cuentas:

a) prestará sus servicios exclusivamente sobre la base del consentimiento explícito del usuario del servicio de pago;

b) garantizará que las credenciales de seguridad personalizadas del usuario de servicios de pago no sean accesibles a terceros, con excepción del usuario y del emisor de las credenciales de seguridad personalizadas, y que, cuando las transmita el proveedor de servicios de pago que preste el servicio de información sobre cuentas, la transmisión se realice a través de canales seguros y eficientes;

c) en cada comunicación, se identificará ante el proveedor o proveedores de servicios de pago gestores de cuenta del usuario de servicios de pago y se comunicará de manera segura con el proveedor o proveedores de servicios de pago gestores de cuenta y el usuario del servicio de pago, de conformidad con lo previsto en el Reglamento Delegado 2018/389 y a los criterios que, dentro de las disposiciones de la Autoridad Bancaria Europea que le resulten aplicables, determine el Banco de España;

d) accederá únicamente a la información de las cuentas de pago designadas por el usuario y las operaciones de pago correspondientes;

e) no solicitará datos de pago sensibles vinculados a las cuentas de pago;

f) no utilizará, almacenará o accederá a ningún dato, para fines distintos de la prestación del servicio de información sobre cuentas expresamente solicitado por el usuario del servicio de pago, de conformidad con las normas sobre protección de datos.

3. En lo que se refiere a las cuentas de pago, el proveedor de servicios de pago gestor de cuenta:

a) establecerá una comunicación segura con los proveedores de servicios de información sobre cuentas, y

b) tratará las peticiones de datos transmitidas a través de los servicios de un proveedor de servicios de pago que preste el servicio de información sobre cuentas sin discriminación alguna, salvo por causas objetivas.

[. . .]

CAPÍTULO IV

Protección de datos

Artículo 65. *Protección de datos.*

1. El tratamiento y cesión de los datos relacionados con las actividades a las que se refiere este real decreto-ley se encuentran sometidos a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y en la normativa española de protección de datos, y en la normativa nacional que lo desarrolla.

[. . .]

§ 34

Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 272, de 9 de noviembre de 2017
Última modificación: 2 de abril de 2025
Referencia: BOE-A-2017-12902

[. . .]

LIBRO PRIMERO

Configuración general de la contratación del sector público y elementos estructurales de los contratos

TÍTULO I

Disposiciones generales sobre la contratación del sector público

[. . .]

CAPÍTULO II

Libertad de pactos y contenido mínimo del contrato

[. . .]

Artículo 35. *Contenido mínimo del contrato.*

1. Los documentos en los que se formalicen los contratos que celebren las entidades del sector público, salvo que ya se encuentren recogidas en los pliegos, deberán incluir, necesariamente, las siguientes menciones:

a) La identificación de las partes.
b) La acreditación de la capacidad de los firmantes para suscribir el contrato.
c) Definición del objeto y tipo del contrato, teniendo en cuenta en la definición del objeto las consideraciones sociales, ambientales y de innovación.
d) Referencia a la legislación aplicable al contrato, con expresa mención al sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.
e) La enumeración de los documentos que integran el contrato. Si así se expresa en el contrato, esta enumeración podrá estar jerarquizada, ordenándose según el orden de

prioridad acordado por las partes, en cuyo supuesto, y salvo caso de error manifiesto, el orden pactado se utilizará para determinar la prevalencia respectiva, en caso de que existan contradicciones entre diversos documentos.

f) El precio cierto, o el modo de determinarlo.

g) La duración del contrato o las fechas estimadas para el comienzo de su ejecución y para su finalización, así como la de la prórroga o prórrogas, si estuviesen previstas.

h) Las condiciones de recepción, entrega o admisión de las prestaciones.

i) Las condiciones de pago.

j) Los supuestos en que procede la modificación, en su caso.

k) Los supuestos en que procede la resolución.

l) El crédito presupuestario o el programa o rúbrica contable con cargo al que se abonará el precio, en su caso.

m) La extensión objetiva y temporal del deber de confidencialidad que, en su caso, se imponga al contratista.

n) La obligación de la empresa contratista de cumplir durante todo el periodo de ejecución de contrato las normas y condiciones fijadas en el convenio colectivo de aplicación.

2. El documento contractual no podrá incluir estipulaciones que establezcan derechos y obligaciones para las partes distintos de los previstos en los pliegos, concretados, en su caso, en la forma que resulte de la proposición del adjudicatario, o de los precisados en el acto de adjudicación del contrato de acuerdo con lo actuado en el procedimiento, de no existir aquellos.

[. . .]

LIBRO SEGUNDO

De los contratos de las Administraciones Públicas

TÍTULO I

Disposiciones generales

CAPÍTULO I

De las actuaciones relativas a la contratación de las Administraciones Públicas

[. . .]

Subsección 2.ª Pliegos de cláusulas administrativas y de prescripciones técnicas

[. . .]

Artículo 122. *Pliegos de cláusulas administrativas particulares.*

1. Los pliegos de cláusulas administrativas particulares deberán aprobarse previamente a la autorización del gasto o conjuntamente con ella, y siempre antes de la licitación del contrato, o de no existir esta, antes de su adjudicación, y solo podrán ser modificados con posterioridad por error material, de hecho o aritmético. En otro caso, la modificación del pliego conllevará la retroacción de actuaciones.

2. En los pliegos de cláusulas administrativas particulares se incluirán los criterios de solvencia y adjudicación del contrato; las consideraciones sociales, laborales y ambientales que como criterios de solvencia, de adjudicación o como condiciones especiales de ejecución se establezcan; los pactos y condiciones definidores de los derechos y obligaciones de las partes del contrato; la previsión de cesión del contrato salvo en los casos en que la misma no sea posible de acuerdo con lo establecido en el segundo párrafo del artículo 214.1; la obligación del adjudicatario de cumplir las condiciones salariales de los trabajadores conforme al Convenio Colectivo sectorial de aplicación; y las demás menciones requeridas por esta Ley y sus normas de desarrollo. En el caso de contratos mixtos, se

detallará el régimen jurídico aplicable a sus efectos, cumplimiento y extinción, atendiendo a las normas aplicables a las diferentes prestaciones fusionadas en ellos.

Téngase en cuenta que se declara que el párrafo primero del apartado 2 no es conforme con el orden constitucional de competencias, salvo los incisos relativos a la necesidad de incluir «los pactos y condiciones definidores de los derechos y obligaciones de las partes del contrato» y «En el caso de contratos mixtos, se detallará el régimen jurídico aplicable a sus efectos, cumplimiento y extinción, atendiendo a las normas aplicables a las diferentes prestaciones fusionadas en ellos», en los términos del fundamento jurídico 7 A) d), por la Sentencia del TC 68/2021, de 18 de marzo. Ref. BOE-A-2021-6614

Los pliegos podrán también especificar si va a exigirse la transferencia de derechos de propiedad intelectual o industrial, sin perjuicio de lo establecido en el artículo 308 respecto de los contratos de servicios.

Los pliegos deberán mencionar expresamente la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos.

Sin perjuicio de lo establecido en el artículo 28.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en aquellos contratos cuya ejecución requiera el tratamiento por el contratista de datos personales por cuenta del responsable del tratamiento, adicionalmente en el pliego se hará constar:

a) La finalidad para la cual se cederán dichos datos.

b) La obligación del futuro contratista de someterse en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos, sin perjuicio de lo establecido en el último párrafo del apartado 1 del artículo 202.

c) La obligación de la empresa adjudicataria de presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos.

d) La obligación de comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere la letra c) anterior.

e) La obligación de los licitadores de indicar en su oferta, si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

En los pliegos correspondientes a los contratos a que se refiere el párrafo anterior las obligaciones recogidas en las letras a) a e) anteriores en todo caso deberán ser calificadas como esenciales a los efectos de lo previsto en la letra f) del apartado 1 del artículo 211.

3. Los pliegos de cláusulas administrativas particulares podrán establecer penalidades, conforme a lo prevenido en el apartado 1 del artículo 192, para los casos de incumplimiento o de cumplimiento defectuoso de la prestación que afecten a características de la misma, en especial cuando se hayan tenido en cuenta para definir los criterios de adjudicación, o atribuir a la puntual observancia de estas características el carácter de obligación contractual esencial a los efectos señalados en la letra f) del apartado 1 del artículo 211. Asimismo, para los casos de incumplimiento de lo prevenido en los artículos 130 y 201.

3 bis. Las Administraciones públicas incorporarán en los pliegos de cláusulas administrativas particulares condiciones especiales de ejecución o criterios de adjudicación dirigidos a la promoción de la igualdad de trato y no discriminación por razón de orientación sexual, identidad sexual, expresión de género y características sexuales, siempre que exista vinculación con el objeto del contrato.

4. Los contratos se ajustarán al contenido de los pliegos de cláusulas administrativas particulares, cuyas cláusulas se consideran parte integrante de los mismos.

5. La aprobación de los pliegos de cláusulas administrativas particulares corresponderá al órgano de contratación, que podrá, asimismo, aprobar modelos de pliegos particulares para determinadas categorías de contratos de naturaleza análoga.

6. La Junta Consultiva de Contratación Pública del Estado deberá informar con carácter previo todos los pliegos de cláusulas administrativas particulares en que se proponga la inclusión de estipulaciones contrarias a los correspondientes pliegos generales.

7. En la Administración General del Estado, sus Organismos Autónomos, Entidades Gestoras y Servicios Comunes de la Seguridad Social y demás Administraciones Públicas integrantes del sector público estatal, la aprobación de los pliegos y de los modelos requerirá el informe previo del Servicio Jurídico respectivo. Este informe no será necesario cuando el pliego de cláusulas administrativas particulares se ajuste a un modelo de pliego que haya sido previamente objeto de este informe.

[. . .]

Sección 2.ª De la adjudicación de los contratos de las Administraciones Públicas

Subsección 1.ª Normas generales

[. . .]

Artículo 133. *Confidencialidad.*

1. Sin perjuicio de lo dispuesto en la legislación vigente en materia de acceso a la información pública y de las disposiciones contenidas en la presente Ley relativas a la publicidad de la adjudicación y a la información que debe darse a los candidatos y a los licitadores, los órganos de contratación no podrán divulgar la información facilitada por los empresarios que estos hayan designado como confidencial en el momento de presentar su oferta. El carácter de confidencial afecta, entre otros, a los secretos técnicos o comerciales, a los aspectos confidenciales de las ofertas y a cualesquiera otras informaciones cuyo contenido pueda ser utilizado para falsear la competencia, ya sea en ese procedimiento de licitación o en otros posteriores.

El deber de confidencialidad del órgano de contratación así como de sus servicios dependientes no podrá extenderse a todo el contenido de la oferta del adjudicatario ni a todo el contenido de los informes y documentación que, en su caso, genere directa o indirectamente el órgano de contratación en el curso del procedimiento de licitación. Únicamente podrá extenderse a documentos que tengan una difusión restringida, y en ningún caso a documentos que sean públicamente accesibles.

El deber de confidencialidad tampoco podrá impedir la divulgación pública de partes no confidenciales de los contratos celebrados, tales como, en su caso, la liquidación, los plazos finales de ejecución de la obra, las empresas con las que se ha contratado y subcontratado, y, en todo caso, las partes esenciales de la oferta y las modificaciones posteriores del contrato, respetando en todo caso lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. El contratista deberá respetar el carácter confidencial de aquella información a la que tenga acceso con ocasión de la ejecución del contrato a la que se le hubiese dado el referido carácter en los pliegos o en el contrato, o que por su propia naturaleza deba ser tratada como tal. Este deber se mantendrá durante un plazo de cinco años desde el conocimiento de esa información, salvo que los pliegos o el contrato establezcan un plazo mayor que, en todo caso, deberá ser definido y limitado en el tiempo.

[. . .]

Sección 3.ª De los efectos, cumplimiento y extinción de los contratos administrativos

[. . .]

Subsección 3.ª Ejecución de los contratos

[. . .]

Artículo 202. *Condiciones especiales de ejecución del contrato de carácter social, ético, medioambiental o de otro orden.*

1. Los órganos de contratación podrán establecer condiciones especiales en relación con la ejecución del contrato, siempre que estén vinculadas al objeto del contrato, en el sentido del artículo 145, no sean directa o indirectamente discriminatorias, sean compatibles con el Derecho de la Unión Europea y se indiquen en el anuncio de licitación y en los pliegos.

En todo caso, será obligatorio el establecimiento en el pliego de cláusulas administrativas particulares de al menos una de las condiciones especiales de ejecución de entre las que enumera el apartado siguiente.

Asimismo en los pliegos correspondientes a los contratos cuya ejecución implique la cesión de datos por las entidades del sector público al contratista será obligatorio el establecimiento de una condición especial de ejecución que haga referencia a la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos, advirtiéndose además al contratista de que esta obligación tiene el carácter de obligación contractual esencial de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211.

Cuando se cumplan las condiciones previstas en el párrafo primero de este apartado, en los pliegos de contratación de servicios de alimentación en instituciones públicas será obligatorio que se incorpore, como condición especial de ejecución, la observancia de prácticas adecuadas desde el punto de vista del desperdicio alimentario y del cumplimiento de la Ley 1/2025, de 1 de abril, de prevención de las pérdidas y el desperdicio alimentario.

2. Estas condiciones de ejecución podrán referirse, en especial, a consideraciones económicas, relacionadas con la innovación, de tipo medioambiental o de tipo social.

En particular, se podrán establecer, entre otras, consideraciones de tipo medioambiental que persigan: la reducción de las emisiones de gases de efecto invernadero, contribuyéndose así a dar cumplimiento al objetivo que establece el artículo 88 de la Ley 2/2011, de 4 de marzo, de Economía Sostenible; el mantenimiento o mejora de los valores medioambientales que puedan verse afectados por la ejecución del contrato; una gestión más sostenible del agua; el fomento del uso de las energías renovables; la promoción del reciclado de productos y el uso de envases reutilizables; o el impulso de la entrega de productos a granel y la producción ecológica.

Las consideraciones de tipo social o relativas al empleo, podrán introducirse, entre otras, con alguna de las siguientes finalidades: hacer efectivos los derechos reconocidos en la Convención de las Naciones Unidas sobre los derechos de las personas con discapacidad; contratar un número de personas con discapacidad superior al que exige la legislación nacional; promover el empleo de personas con especiales dificultades de inserción en el mercado laboral, en particular de las personas con discapacidad o en situación o riesgo de exclusión social a través de Empresas de Inserción; eliminar las desigualdades entre el hombre y la mujer en dicho mercado, favoreciendo la aplicación de medidas que fomenten la igualdad entre mujeres y hombres en el trabajo; favorecer la mayor participación de la mujer en el mercado laboral y la conciliación del trabajo y la vida familiar; combatir el paro, en particular el juvenil, el que afecta a las mujeres y el de larga duración; favorecer la formación en el lugar de trabajo; garantizar la seguridad y la protección de la salud en el lugar de trabajo y el cumplimiento de los convenios colectivos sectoriales y territoriales aplicables; medidas para prevenir la siniestralidad laboral; otras finalidades que se establezcan con referencia a la estrategia coordinada para el empleo, definida en el artículo 145 del Tratado de Funcionamiento de la Unión Europea; o garantizar el respeto a los derechos laborales básicos a lo largo de la cadena de producción mediante la exigencia del cumplimiento de las Convenciones fundamentales de la Organización Internacional del Trabajo, incluidas aquellas consideraciones que busquen favorecer a los pequeños productores de países en desarrollo, con los que se mantienen relaciones comerciales que les son favorables tales como el pago de un precio mínimo y una prima a los productores o una mayor transparencia y trazabilidad de toda la cadena comercial.

3. Los pliegos podrán establecer penalidades, conforme a lo previsto en el apartado 1 del artículo 192, para el caso de incumplimiento de estas condiciones especiales de ejecución, o atribuirles el carácter de obligaciones contractuales esenciales a los efectos señalados en la letra f) del artículo 211. Cuando el incumplimiento de estas condiciones no se tipifique como

causa de resolución del contrato, el mismo podrá ser considerado en los pliegos, en los términos que se establezcan reglamentariamente, como infracción grave a los efectos establecidos en la letra c) del apartado 2 del artículo 71.

4. Todas las condiciones especiales de ejecución que formen parte del contrato serán exigidas igualmente a todos los subcontratistas que participen de la ejecución del mismo.

[. . .]

Subsección 5.ª Suspensión y extinción de los contratos

[. . .]

Artículo 215. *Subcontratación.*

1. El contratista podrá concertar con terceros la realización parcial de la prestación con sujeción a lo que dispongan los pliegos, salvo que conforme a lo establecido en las letras d) y e) del apartado 2.º de este artículo, la prestación o parte de la misma haya de ser ejecutada directamente por el primero.

En ningún caso la limitación de la subcontratación podrá suponer que se produzca una restricción efectiva de la competencia, sin perjuicio de lo establecido en la presente Ley respecto a los contratos de carácter secreto o reservado, o aquellos cuya ejecución deba ir acompañada de medidas de seguridad especiales de acuerdo con disposiciones legales o reglamentarias o cuando lo exija la protección de los intereses esenciales de la seguridad del Estado.

2. La celebración de los subcontratos estará sometida al cumplimiento de los siguientes requisitos:

a) Si así se prevé en los pliegos, los licitadores deberán indicar en la oferta la parte del contrato que tengan previsto subcontratar, señalando su importe, y el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

b) En todo caso, el contratista deberá comunicar por escrito, tras la adjudicación del contrato y, a más tardar, cuando inicie la ejecución de este, al órgano de contratación la intención de celebrar los subcontratos, señalando la parte de la prestación que se pretende subcontratar y la identidad, datos de contacto y representante o representantes legales del subcontratista, y justificando suficientemente la aptitud de este para ejecutarla por referencia a los elementos técnicos y humanos de que dispone y a su experiencia, y acreditando que el mismo no se encuentra incurso en prohibición de contratar de acuerdo con el artículo 71.

El contratista principal deberá notificar por escrito al órgano de contratación cualquier modificación que sufra esta información durante la ejecución del contrato principal, y toda la información necesaria sobre los nuevos subcontratistas.

En el caso que el subcontratista tuviera la clasificación adecuada para realizar la parte del contrato objeto de la subcontratación, la comunicación de esta circunstancia será suficiente para acreditar la aptitud del mismo.

La acreditación de la aptitud del subcontratista podrá realizarse inmediatamente después de la celebración del subcontrato si esta es necesaria para atender a una situación de emergencia o que exija la adopción de medidas urgentes y así se justifica suficientemente.

c) Si los pliegos hubiesen impuesto a los licitadores la obligación de comunicar las circunstancias señaladas en la letra a) del presente apartado, los subcontratos que no se ajusten a lo indicado en la oferta, por celebrarse con empresarios distintos de los indicados nominativamente en la misma o por referirse a partes de la prestación diferentes a las señaladas en ella, no podrán celebrarse hasta que transcurran veinte días desde que se hubiese cursado la notificación y aportado las justificaciones a que se refiere la letra b) de este apartado, salvo que con anterioridad hubiesen sido autorizados expresamente, siempre que la Administración no hubiese notificado dentro de este plazo su oposición a los mismos. Este régimen será igualmente aplicable si los subcontratistas hubiesen sido identificados en la oferta mediante la descripción de su perfil profesional.

Bajo la responsabilidad del contratista, los subcontratos podrán concluirse sin necesidad de dejar transcurrir el plazo de veinte días si su celebración es necesaria para atender a una

situación de emergencia o que exija la adopción de medidas urgentes y así se justifica suficientemente.

d) En los contratos de carácter secreto o reservado, o en aquellos cuya ejecución deba ir acompañada de medidas de seguridad especiales de acuerdo con disposiciones legales o reglamentarias o cuando lo exija la protección de los intereses esenciales de la seguridad del Estado, la subcontratación requerirá siempre autorización expresa del órgano de contratación.

e) De conformidad con lo establecido en el apartado 4 del artículo 75, en los contratos de obras, los contratos de servicios o los servicios o trabajos de colocación o instalación en el contexto de un contrato de suministro, los órganos de contratación podrán establecer en los pliegos que determinadas tareas críticas no puedan ser objeto de subcontratación, debiendo ser estas ejecutadas directamente por el contratista principal. La determinación de las tareas críticas deberá ser objeto de justificación en el expediente de contratación.

3. La infracción de las condiciones establecidas en el apartado anterior para proceder a la subcontratación, así como la falta de acreditación de la aptitud del subcontratista o de las circunstancias determinantes de la situación de emergencia o de las que hacen urgente la subcontratación, tendrá, entre otras previstas en esta Ley, y en función de la repercusión en la ejecución del contrato, alguna de las siguientes consecuencias, cuando así se hubiera previsto en los pliegos:

a) La imposición al contratista de una penalidad de hasta un 50 por 100 del importe del subcontrato.

b) La resolución del contrato, siempre y cuando se cumplan los requisitos establecidos en el segundo párrafo de la letra f) del apartado 1 del artículo 211.

4. Los subcontratistas quedarán obligados solo ante el contratista principal que asumirá, por tanto, la total responsabilidad de la ejecución del contrato frente a la Administración, con arreglo estricto a los pliegos de cláusulas administrativas particulares o documento descriptivo, y a los términos del contrato; incluido el cumplimiento de las obligaciones en materia medioambiental, social o laboral a que se refiere el artículo 201, así como de la obligación a que hace referencia el último párrafo del apartado 1 del artículo 202 referida al sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.

El conocimiento que tenga la Administración de los subcontratos celebrados en virtud de las comunicaciones a que se refieren las letras b) y c) del apartado 2 de este artículo, o la autorización que otorgue en el supuesto previsto en la letra d) de dicho apartado, no alterarán la responsabilidad exclusiva del contratista principal.

5. En ningún caso podrá concertarse por el contratista la ejecución parcial del contrato con personas inhabilitadas para contratar de acuerdo con el ordenamiento jurídico o comprendidas en alguno de los supuestos del artículo 71.

6. El contratista deberá informar a los representantes de los trabajadores de la subcontratación, de acuerdo con la legislación laboral.

7. Los subcontratos y los contratos de suministro a que se refieren los artículos 215 a 217 tendrán en todo caso naturaleza privada.

8. Sin perjuicio de lo establecido en la disposición adicional quincuagésima primera los subcontratistas no tendrán acción directa frente a la Administración contratante por las obligaciones contraídas con ellos por el contratista como consecuencia de la ejecución del contrato principal y de los subcontratos.

[. . .]

LIBRO CUARTO

Organización administrativa para la gestión de la contratación

[. . .]

TÍTULO II

Registros Oficiales

[. . .]

CAPÍTULO II

Registro de Contratos del Sector Público

Artículo 346. *Registro de Contratos del Sector Público.*

1. El Ministerio de Hacienda y Función Pública mantendrá un Registro de Contratos, en el que se inscribirán los datos básicos de los contratos adjudicados por las distintas Administraciones Públicas y demás entidades del sector público sujetas a esta Ley.

2. El Registro de Contratos del Sector Público constituye el sistema oficial central de información sobre la contratación pública en España. La información sobre la contratación pública deberá estar sistematizada siguiendo formatos y estándares abiertos adoptados a nivel internacional.

3. Los poderes adjudicadores comunicarán al Registro de Contratos del Sector Público, para su inscripción, los datos básicos de los contratos por ellos adjudicados, entre los que figurará la identidad del adjudicatario, el importe de adjudicación de los mismos, junto con el desglose correspondiente del Impuesto sobre el Valor Añadido.

Igualmente comunicarán, en su caso, las modificaciones, prórrogas, variaciones de plazos o de precio, importe final y extinción de aquellos. El contenido y el formato de dichas comunicaciones, así como el plazo para efectuarlas, se establecerán reglamentariamente.

Se exceptuarán de la comunicación señalada en este apartado los contratos excluidos por la presente Ley y aquellos cuyo precio fuera inferior a cinco mil euros, IVA incluido, siempre que el sistema de pago utilizado por los poderes adjudicadores fuera el de anticipo de caja fija u otro sistema similar para realizar pagos menores. En el resto de contratos inferiores a cinco mil euros, deberá comunicarse el órgano de contratación, denominación u objeto del contrato, adjudicatario, número o código identificativo del contrato e importe final.

4. Las comunicaciones de datos de contratos al Registro de Contratos del Sector Público se efectuarán por medios electrónicos, informáticos o telemáticos, en la forma que determine el Ministro de Hacienda y Función Pública.

5. El Registro de Contratos del Sector Público facilitará de modo telemático el acceso a sus datos a los órganos de las Administraciones Públicas que los precisen para el ejercicio de sus competencias legalmente atribuidas.

Asimismo, de conformidad con lo establecido en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, y con las limitaciones que imponen las normas sobre protección de datos de carácter personal, facilitará el acceso público a los datos que no tengan el carácter de confidenciales y que no hayan sido previamente publicados de modo telemático y a través de Internet.

6. En los casos de Administraciones Públicas que dispongan de Registros de Contratos análogos en su ámbito de competencias, la comunicación de datos a que se refiere el apartado 3 del presente artículo podrá ser sustituida por comunicaciones entre los respectivos Registros de Contratos. El Ministerio de Hacienda y Función Pública determinará las especificaciones y requisitos para el intercambio de datos entre el Registro de Contratos del Sector Público y los demás Registros de Contratos.

7. Al objeto de garantizar la identificación única y precisa de cada contrato, las Administraciones y entidades comunicantes asignarán a cada uno de ellos un código identificador, que será único en su ámbito de competencias. El Ministerio de Hacienda y Función Pública determinará las reglas de asignación de dichos identificadores únicos que resulten necesarios para asegurar la identificación unívoca de cada contrato dentro del Registro de Contratos del Sector Público, así como para su coordinación con los demás Registros de Contratos.

8. El Gobierno elevará anualmente a las Cortes Generales un informe sobre la contratación pública en España, a partir de los datos y análisis proporcionados por el Registro de Contratos del Sector Público.

El Ministerio de Hacienda y Función Pública pondrá en conocimiento de la Comisión Nacional de los Mercados y la Competencia el informe al que se refiere el párrafo anterior, tras su elevación por el Gobierno a las Cortes Generales.

[. . .]

Disposición adicional vigésima quinta. *Protección de datos de carácter personal.*

1. Los contratos regulados en la presente Ley que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo.

2. Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquel tendrá la consideración de encargado del tratamiento.

En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 12.2 y 3 de la Ley Orgánica 15/1999, de 13 de diciembre. En todo caso, las previsiones del artículo 12.2 de dicha Ley deberán de constar por escrito.

Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que esta hubiese designado.

El tercero encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.

3. En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:

a) Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.

b) Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.

c) Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

En estos casos, el tercero tendrá también la consideración de encargado del tratamiento.

[. . .]

§ 35

Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 268, de 4 de noviembre de 2017
Última modificación: 3 de enero de 2025
Referencia: BOE-A-2017-12659

[. . .]

TÍTULO II

Obligaciones de las entidades de resolución alternativa acreditadas

[. . .]

Artículo 36. *Garantías de confidencialidad y de protección de datos de carácter personal.*

1. Las entidades acreditadas garantizarán que los procedimientos de resolución alternativa de litigios que gestionen sean confidenciales.

A estos efectos, y entre otras actuaciones, velarán para que tanto las personas encargadas de la decisión del litigio, sujetas al secreto profesional, como las partes en litigio, no revelen la información que hubieran podido obtener con ocasión del procedimiento.

2. Las entidades acreditadas adoptarán las medidas necesarias para asegurar que el tratamiento de los datos personales cumpla con lo establecido en la normativa vigente en materia de protección de datos de carácter personal.

Esta obligación se extenderá al tratamiento de datos llevado a cabo con ocasión de la tramitación de los procedimientos de resolución alternativa como consecuencia de las cesiones que se efectúen en el marco de la cooperación e intercambio de información de las entidades acreditadas o sus redes y en el intercambio de información con autoridades y administraciones públicas.

3. La infracción del deber de confidencialidad por las entidades acreditadas o por las personas encargadas de la decisión del litigio generará la responsabilidad prevista en el ordenamiento jurídico.

Artículo 37. *Actualización de información.*

Las entidades acreditadas trasladarán a la autoridad competente que corresponda, dentro del plazo de 15 días laborables, cualquier modificación que afecte a los datos

comunicados por las mismas, así como a los requisitos, obligaciones y garantías exigidas en esta ley.

[. . .]

§ 36

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. [Inclusión parcial]

Ministerio de Empleo y Seguridad Social
«BOE» núm. 255, de 24 de octubre de 2015
Última modificación: 2 de abril de 2025
Referencia: BOE-A-2015-11430

[. . .]

TÍTULO I

De la relación individual de trabajo

CAPÍTULO I

Disposiciones generales

[. . .]

Artículo 8. *Forma del contrato.*

1. El contrato de trabajo se podrá celebrar por escrito o de palabra. Se presumirá existente entre todo el que presta un servicio por cuenta y dentro del ámbito de organización y dirección de otro y el que lo recibe a cambio de una retribución a aquel.

2. Deberán constar por escrito los contratos de trabajo cuando así lo exija una disposición legal y, en todo caso, los de prácticas y para la formación y el aprendizaje, los contratos a tiempo parcial, fijos-discontinuos y de relevo y los contratos para la realización de una obra o servicio determinado; también constarán por escrito los contratos por tiempo determinado cuya duración sea superior a cuatro semanas.

Deberán constar igualmente por escrito los contratos de trabajo de los pescadores, de los trabajadores que trabajen a distancia y de los trabajadores contratados en España al servicio de empresas españolas en el extranjero.

De no observarse la exigencia de forma escrita, el contrato de trabajo se presumirá celebrado por tiempo indefinido y a jornada completa, salvo prueba en contrario que acredite su naturaleza temporal o el carácter a tiempo parcial de los servicios.

Cualquiera de las partes podrá exigir que el contrato se formalice por escrito, incluso durante el transcurso de la relación laboral.

3. El empresario está obligado a comunicar a la oficina pública de empleo, en el plazo de los diez días siguientes a su concertación y en los términos que reglamentariamente se determinen, el contenido de los contratos de trabajo que celebre o las prórrogas de los mismos, deban o no formalizarse por escrito.

4. El empresario entregará a la representación legal de los trabajadores una copia básica de todos los contratos que deban celebrarse por escrito, a excepción de los contratos de relación laboral especial de alta dirección sobre los que se establece el deber de notificación a la representación legal de los trabajadores.

Con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, esta copia básica contendrá todos los datos del contrato a excepción del número del documento nacional de identidad o del número de identidad de extranjero, el domicilio, el estado civil, y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pudiera afectar a la intimidad personal. El tratamiento de la información facilitada estará sometido a los principios y garantías previstos en la normativa aplicable en materia de protección de datos.

La copia básica se entregará por el empresario, en plazo no superior a diez días desde la formalización del contrato, a los representantes legales de los trabajadores, quienes la firmarán a efectos de acreditar que se ha producido la entrega.

Posteriormente, dicha copia básica se enviará a la oficina de empleo. Cuando no exista representación legal de los trabajadores también deberá formalizarse copia básica y remitirse a la oficina de empleo.

Los representantes de la Administración, así como los de las organizaciones sindicales y de las asociaciones empresariales, que tengan acceso a la copia básica de los contratos en virtud de su pertenencia a los órganos de participación institucional que reglamentariamente tengan tales facultades, observarán sigilo profesional, no pudiendo utilizar dicha documentación para fines distintos de los que motivaron su conocimiento.

5. Cuando la relación laboral sea de duración superior a cuatro semanas, el empresario deberá informar por escrito al trabajador, en los términos y plazos que se establezcan reglamentariamente, sobre los elementos esenciales del contrato y las principales condiciones de ejecución de la prestación laboral, siempre que tales elementos y condiciones no figuren en el contrato de trabajo formalizado por escrito.

[. . .]

CAPÍTULO II

Contenido del contrato de trabajo

[. . .]

Artículo 20 bis. *Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.*

Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

[. . .]

§ 37

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 236, de 2 de octubre de 2015
Última modificación: 2 de agosto de 2024
Referencia: BOE-A-2015-10566

TÍTULO PRELIMINAR

Disposiciones generales, principios de actuación y funcionamiento del sector público

CAPÍTULO I

Disposiciones generales

[. . .]

Artículo 3. *Principios generales.*

1. Las Administraciones Públicas sirven con objetividad los intereses generales y actúan de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Constitución, a la Ley y al Derecho.

Deberán respetar en su actuación y relaciones los siguientes principios:

a) Servicio efectivo a los ciudadanos.
b) Simplicidad, claridad y proximidad a los ciudadanos.
c) Participación, objetividad y transparencia de la actuación administrativa.
d) Racionalización y agilidad de los procedimientos administrativos y de las actividades materiales de gestión.
e) Buena fe, confianza legítima y lealtad institucional.
f) Responsabilidad por la gestión pública.
g) Planificación y dirección por objetivos y control de la gestión y evaluación de los resultados de las políticas públicas.
h) Eficacia en el cumplimiento de los objetivos fijados.
i) Economía, suficiencia y adecuación estricta de los medios a los fines institucionales.
j) Eficiencia en la asignación y utilización de los recursos públicos.
k) Cooperación, colaboración y coordinación entre las Administraciones Públicas.

2. Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada

una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

3. Bajo la dirección del Gobierno de la Nación, de los órganos de gobierno de las Comunidades Autónomas y de los correspondientes de las Entidades Locales, la actuación de la Administración Pública respectiva se desarrolla para alcanzar los objetivos que establecen las leyes y el resto del ordenamiento jurídico.

4. Cada una de las Administraciones Públicas del artículo 2 actúa para el cumplimiento de sus fines con personalidad jurídica única.

[. . .]

CAPÍTULO V

Funcionamiento electrónico del sector público

Artículo 38. *La sede electrónica.*

1. La sede electrónica es aquella dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a una o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.

2. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

3. Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del órgano titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.

4. Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

5. La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y uso de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

6. Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, certificados reconocidos o cualificados de autenticación de sitio web o medio equivalente.

Artículo 39. *Portal de internet.*

Se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de Derecho Público que permite el acceso a través de internet a la información publicada y, en su caso, a la sede electrónica correspondiente.

Artículo 40. *Sistemas de identificación de las Administraciones Públicas.*

1. Las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

2. Se entenderá identificada la Administración Pública respecto de la información que se publique como propia en su portal de internet.

Artículo 41. *Actuación administrativa automatizada.*

1. Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público.

2. En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

Artículo 42. *Sistemas de firma para la actuación administrativa automatizada.*

En el ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Artículo 43. *Firma electrónica del personal al servicio de las Administraciones Públicas.*

1. Sin perjuicio de lo previsto en los artículos 38, 41 y 42, la actuación de una Administración Pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano o empleado público.

2. Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios. Por razones de seguridad pública los sistemas de firma electrónica podrán referirse sólo el número de identificación profesional del empleado público.

Artículo 44. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos, organismos públicos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en este artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a una misma Administración Pública, ésta determinará las condiciones y garantías por las que se regirá que, al menos, comprenderá la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas Administraciones, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio suscrito entre aquellas.

4. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

Artículo 45. *Aseguramiento e interoperabilidad de la firma electrónica.*

1. Las Administraciones Públicas podrán determinar los trámites e informes que incluyan firma electrónica reconocida o cualificada y avanzada basada en certificados electrónicos reconocidos o cualificados de firma electrónica.

2. Con el fin de favorecer la interoperabilidad y posibilitar la verificación automática de la firma electrónica de los documentos electrónicos, cuando una Administración utilice sistemas

de firma electrónica distintos de aquellos basados en certificado electrónico reconocido o cualificado, para remitir o poner a disposición de otros órganos, organismos públicos, entidades de Derecho Público o Administraciones la documentación firmada electrónicamente, podrá superponer un sello electrónico basado en un certificado electrónico reconocido o cualificado.

Artículo 46. *Archivo electrónico de documentos.*

1. Todos los documentos utilizados en las actuaciones administrativas se almacenarán por medios electrónicos, salvo cuando no sea posible.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones Públicas que así lo requieran, de acuerdo con las especificaciones sobre el ciclo de vida de los servicios y sistemas utilizados.

Artículo 46 bis. *Ubicación de los sistemas de información y comunicaciones para el registro de datos.*

Los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, deberán ubicarse y prestarse dentro del territorio de la Unión Europea.

Los datos a que se refiere el apartado anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

[. . .]

§ 38

Acuerdo de 23 de julio de 2015, del Pleno del Tribunal Constitucional, por el que se regula la exclusión de los datos de identidad personal en la publicación de las resoluciones jurisdiccionales

Tribunal Constitucional
«BOE» núm. 178, de 27 de julio de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-8372

El Pleno del Tribunal Constitucional, en ejercicio de la competencia definida en el artículo 2.2, en relación con el artículo 10.1.m), de la Ley Orgánica 2/1979, de 3 de octubre, ha adoptado el siguiente acuerdo:

Artículo 1.

El Tribunal Constitucional en sus resoluciones jurisdiccionales preservará de oficio el anonimato de los menores y personas que requieran un especial deber de tutela, de las víctimas de delitos de cuya difusión se deriven especiales perjuicios y de las personas que no estén constituidas en parte en el proceso constitucional.

Artículo 2.

El Tribunal, en los demás casos, podrá excepcionar, de oficio o a instancia de parte, la exigencia constitucional de publicidad de sus resoluciones (artículo 164 CE), en lo relativo a los datos de identidad y situación personal de las partes intervinientes en el proceso.

A tal fin, si una parte estimase necesario que en un asunto sometido al conocimiento del Tribunal no se divulgue públicamente su identidad o situación personal, deberá solicitarlo en el momento de formular la demanda o en el de su personación, exponiendo los motivos de su petición.

El Tribunal accederá a la petición cuando, a partir de la ponderación de circunstancias debidamente acreditadas concurrentes en el caso, la estime justificada por resultar prevalente el derecho a la intimidad u otros intereses constitucionales.

Artículo 3.

En los casos en que proceda preservar el anonimato de las personas concernidas por la publicación de las resoluciones del Tribunal Constitucional, se sustituirá su identidad por las iniciales correspondientes y se omitirán los demás datos que permitan su identificación.

Disposición transitoria.

Las disposiciones de este acuerdo serán aplicables a los procesos iniciados antes de su entrada en vigor.

Disposición final.

El presente acuerdo entrará en vigor el día de su publicación en el «Boletín oficial del Estado».

§ 39

Ley 23/2015, de 21 de julio, Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 174, de 22 de julio de 2015
Última modificación: 3 de enero de 2025
Referencia: BOE-A-2015-8168

[. . .]

TÍTULO II

Funcionamiento del Sistema

CAPÍTULO I

De las funciones de la Inspección de Trabajo y Seguridad Social

[. . .]

Artículo 16. *Auxilio y colaboración con la Inspección de Trabajo y Seguridad Social.*

1. Las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos de la Administración General del Estado, de las Administraciones de las Comunidades Autónomas y de las Entidades Locales; los organismos autónomos y las entidades públicas empresariales; las cámaras y corporaciones, colegios y asociaciones profesionales; las demás entidades públicas, y quienes, en general, ejerzan funciones públicas, estarán obligados a suministrar a la Inspección de Trabajo y Seguridad Social cuantos datos, informes y antecedentes que tengan trascendencia en el ámbito de sus competencias, así como a prestarle la colaboración que le sea solicitada para el ejercicio de la función inspectora.

2. El Consejo General del Notariado suministrará a la Inspección de Trabajo y Seguridad Social, de forma telemática, la información contenida en el índice único informatizado regulado en el artículo 17 de la Ley del Notariado de 28 de mayo de 1862, que tenga trascendencia en el ejercicio de la función inspectora.

3. La Administración Tributaria cederá sus datos y antecedentes a la Inspección de Trabajo y Seguridad Social en los términos establecidos en el artículo 95.1.c) de la Ley 58/2003, de 17 de diciembre, General Tributaria. Asimismo, las entidades gestoras y colaboradoras y los servicios comunes de la Seguridad Social prestarán su colaboración a la Inspección de Trabajo y Seguridad Social, facilitándole, cuando le sean solicitadas, las informaciones, antecedentes y datos con relevancia en el ejercicio de la función inspectora, incluso los de carácter personal objeto de tratamiento automatizado, sin necesidad de consentimiento del afectado. La Administración Tributaria y la Inspección de Trabajo y

Seguridad Social establecerán programas de mutua correspondencia y de coordinación para el cumplimiento de sus fines.

4. Los órganos de la Administración General del Estado y los de las Comunidades Autónomas colaborarán con la Inspección de Trabajo y Seguridad Social y le prestarán el apoyo y el asesoramiento pericial y técnico necesario.

5. Las mutualidades de previsión social deberán colaborar y suministrar a la Inspección de Trabajo y Seguridad Social los datos e informes que resulten necesarios para el adecuado desarrollo de la actividad de la Inspección, en lo relativo a su condición de entidad alternativa al Régimen Especial de la Seguridad Social de los Trabajadores por Cuenta Propia o Autónomos.

6. Las obligaciones de auxilio y colaboración establecidas en los apartados anteriores sólo tendrán las limitaciones legalmente establecidas referentes a la intimidad de la persona, al secreto de la correspondencia, o de las informaciones suministradas a las Administraciones Públicas con finalidad exclusivamente estadística.

7. Las autoridades competentes en materia de transporte terrestre facilitarán a la Inspección de Trabajo y Seguridad Social la información de que dispongan con trascendencia en el ejercicio de la función inspectora y, en particular, la necesaria para la vigilancia, en el ámbito de sus competencias, del cumplimiento de lo previsto en el capítulo V de la Ley 45/1999, de 29 de noviembre, sobre desplazamiento de trabajadores en el marco de una prestación de servicios transnacional.

8. Las Fuerzas y Cuerpos de Seguridad competentes estarán obligadas a prestar apoyo, auxilio y colaboración a la Inspección de Trabajo y Seguridad Social en el desempeño de sus funciones, a través de los mandos designados a tal efecto por la autoridad correspondiente.

9. Mediante convenios u otros instrumentos se establecerán las formas de colaboración con la Inspección de Trabajo y Seguridad Social por parte de otros órganos de la Administración General del Estado o de otras Administraciones Públicas para los supuestos en que, como consecuencia de su actuación, tengan conocimiento de hechos presuntamente constitutivos de trabajo no declarado y empleo irregular.

Los hechos comprobados directamente por los funcionarios que ostenten la condición de Autoridad o de agentes de ella, contenidos en comunicaciones que se formulen en ejecución de lo establecido en los convenios o instrumentos indicados en el párrafo anterior, tras su valoración y calificación por la Inspección de Trabajo y Seguridad Social, podrán ser aducidos como prueba en los procedimientos iniciados por esta y serán tenidos por ciertos, salvo prueba en contrario de los interesados.

10. Los Juzgados y Tribunales facilitarán a la Inspección de Trabajo y Seguridad Social, de oficio o a petición de la misma, los datos de trascendencia para la función inspectora que se desprendan de las actuaciones en que conozcan y que no resulten afectados por el secreto sumarial.

11. La colaboración de las Autoridades de los Estados Miembros de la Unión Europea con competencias equivalentes a las de la Inspección de Trabajo y Seguridad Social se regirá por la normativa de la Unión Europea o por los instrumentos o acuerdos bilaterales o multilaterales de los que sea parte el Estado Español.

Los hechos comprobados por dichas autoridades en el ámbito de la cooperación administrativa internacional que sean facilitados a las autoridades españolas podrán ser aducidos como prueba por la Inspección de Trabajo y Seguridad Social en los procedimientos iniciados por esta y serán tenidos por ciertos, salvo prueba en contrario de los interesados.

12. La obtención de datos de carácter personal no recabados del interesado por los funcionarios de la Inspección en el ejercicio de sus competencias, no requerirá la información expresa e inequívoca a los interesados prevista en el artículo 5.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[. . .]

Artículo 18. *De la colaboración con los funcionarios de la Inspección de Trabajo y Seguridad Social.*

1. Los empresarios, los trabajadores y los representantes de ambos, así como los demás sujetos responsables del cumplimiento de las normas del orden social, están obligados cuando sean requeridos:

a) A atender debidamente a los inspectores de Trabajo y Seguridad Social y a los Subinspectores Laborales.

b) A acreditar su identidad y la de quienes se encuentren en los centros de trabajo.

c) A colaborar con ellos con ocasión de visitas u otras actuaciones inspectoras.

d) A declarar ante el funcionario actuante sobre cuestiones que afecten a las comprobaciones inspectoras, así como a facilitarles la información y documentación necesarias para el desarrollo de sus funciones. Quienes representen a los sujetos inspeccionados deberán acreditar documentalmente tal condición si la actuación se produjese fuera del domicilio o centro de trabajo visitado.

2. Toda persona natural o jurídica estará obligada a proporcionar a la Inspección de Trabajo y Seguridad Social toda clase de datos, antecedentes o información con trascendencia en los cometidos inspectores, siempre que se deduzcan de sus relaciones económicas, profesionales, empresariales o financieras con terceros sujetos a la acción inspectora, cuando a ello sea requerida en forma. Tal obligación alcanza a las entidades colaboradoras de los órganos de recaudación de la Seguridad Social y a las depositarias de dinero en efectivo o de fondos en cuanto a la identificación de pagos realizados con cargo a las cuentas que pueda tener en dicha entidad la persona que se señale en el correspondiente requerimiento, sin que puedan ampararse en el secreto bancario. La obligación de los profesionales de facilitar información no alcanza a aquellos datos confidenciales a que hubieran accedido por su prestación de servicios de asesoramiento y defensa o con ocasión de prestaciones o atenciones sanitarias, salvo conformidad previa y expresa de los interesados. El incumplimiento de estos requerimientos se considerará como infracción por obstrucción conforme al texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, aprobado por el Real Decreto Legislativo 5/2000, de 4 de agosto. Reglamentariamente se determinará la forma y requisitos aplicables a los referidos requerimientos.

3. La colaboración con la Inspección de Trabajo y Seguridad Social se llevará a efecto, preferentemente, por medios electrónicos, conforme a lo dispuesto en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

4. De conformidad con lo previsto en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre, la transmisión a la Inspección de aquellos datos personales que sean necesarios para el ejercicio de la función inspectora, en virtud de su deber de colaboración, no estará sujeta a la necesidad de consentimiento del interesado.

Los datos que hubieran sido transmitidos únicamente se emplearán para ejercicio de las competencias atribuidas por esta ley a la Inspección de Trabajo y Seguridad Social.

CAPÍTULO II

De las actuaciones de la Inspección de Trabajo y Seguridad Social

[. . .]

Artículo 24. *Información del Sistema de Inspección de Trabajo y Seguridad Social.*

1. Conforme al principio de concepción única e integral del Sistema de Inspección de Trabajo y Seguridad Social, deberá garantizarse en el tratamiento de la información de dicho Sistema la unidad e integración de la información, la interoperabilidad, la interconexión y el acceso a la misma a las distintas Administraciones Públicas en función de las materias objeto de su competencia, en los términos establecidos en esta ley y su normativa de desarrollo.

En consecuencia, el personal del Sistema de Inspección de Trabajo y Seguridad Social, podrá acceder a la información necesaria para el ejercicio de las funciones inspectoras, de

los registros y bases de datos disponibles, de acuerdo con lo dispuesto en el artículo 16 y en los términos que se establezcan.

2. El tratamiento de la información del Sistema debe realizarse a partir de una base de datos unitaria e integrada, que mantenga la homogeneidad de los datos y consolide, en el conjunto del Estado, la información aportada por los servicios de la Inspección de Trabajo y Seguridad Social, así como la que se derive de sus actuaciones.

3. El tratamiento de los datos de carácter personal incorporados a la base de datos del Sistema se encuentra sujeto a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

No obstante, no será necesario el consentimiento de los interesados para la inclusión de sus datos en la base de datos del Sistema ni para el acceso a los mismos o su comunicación a terceros por parte de las Administraciones Públicas competentes.

4. Serán de aplicación al sistema de información las medidas de seguridad de nivel alto establecidas en la normativa de protección de datos de carácter personal.

[. . .]

Disposición adicional undécima. *Régimen de incompatibilidades.*

El personal funcionario previsto en el artículo 3 de esta ley, podrá realizar actividades de conciliación, mediación y arbitraje en huelgas y otros conflictos laborales ajenas a la función inspectora, en el ámbito de los sistemas autónomos de solución de conflictos laborales constituidos mediante los acuerdos interprofesionales o los convenios colectivos a los que se refiere el artículo 83 del Estatuto de los Trabajadores, de acuerdo con las normas reguladoras del funcionamiento de los mismos, así como funciones arbitrales previstas en el artículo 76 del texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, siempre que estas actividades no tengan carácter permanente.

Dichas actividades quedan exceptuadas del régimen de incompatibilidades previsto en la Ley 53/1984, de 26 de diciembre, de incompatibilidades al servicio de las Administraciones públicas.

Téngase en cuenta que esta disposición, añadida por la disposición final 25 de la Ley Orgánica 1/2025, de 2 de enero, Ref. BOE-A-2025-76, entra en vigor el 3 de abril de 2025 según establece su disposición final 38.1

[. . .]

§ 40

Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 77, de 31 de marzo de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-3444

[. . .]

TÍTULO III

Órganos de vigilancia y control de los altos cargos de la Administración General del Estado

[. . .]

Artículo 21. *Registros.*

1. Los Registros electrónicos de Actividades y de Bienes y Derechos Patrimoniales de Altos Cargos se alojarán en un sistema de gestión documental que garantice la inalterabilidad y permanencia de sus datos, así como la alta seguridad en el acceso y uso de éstos.

2. El Registro electrónico de Actividades tendrá carácter público, rigiéndose por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en la Ley 19/2013, de 9 de diciembre, en esta ley y en las normas de desarrollo de las leyes citadas.

3. El Registro electrónico de Bienes y Derechos Patrimoniales tendrá carácter reservado y solo podrán tener acceso al mismo además del propio interesado, los siguientes órganos:

a) El Congreso de los Diputados y el Senado, de acuerdo con lo que establezcan los reglamentos de las Cámaras, así como las comisiones parlamentarias de investigación que se constituyan.

b) Los órganos judiciales para la instrucción o resolución de procesos que requieran el conocimiento de los datos que obran en el Registro, de conformidad con lo dispuesto en las leyes procesales.

c) El Ministerio Fiscal cuando realice actuaciones de investigación en el ejercicio de sus funciones que requieran el conocimiento de los datos obrantes en el Registro.

4. Los órganos mencionados en el apartado anterior adoptarán las medidas necesarias para mantener el carácter reservado de la información contenida en el Registro electrónico de Bienes y Derechos Patrimoniales, sin perjuicio de la aplicación de las normas reguladoras de los procedimientos en cuya tramitación se hubiera solicitado la información.

5. El contenido de las declaraciones de bienes y derechos patrimoniales de los miembros del Gobierno y de los Secretarios de Estado y demás Altos Cargos se publicarán en el

«Boletín Oficial del Estado», en los términos previstos reglamentariamente. En relación con los bienes patrimoniales, se publicará una declaración comprensiva de la situación patrimonial de estos Altos Cargos, omitiéndose aquellos datos referentes a su localización y salvaguardando la privacidad y seguridad de sus titulares.

[. . .]

§ 41

Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 156, de 27 de junio de 2014
Última modificación: 29 de junio de 2023
Referencia: BOE-A-2014-6726

TÍTULO I

De las entidades de crédito

CAPÍTULO I

Disposiciones generales

[. . .]

Artículo 5. *Protección del cliente de entidades de crédito.*

1. Las entidades de crédito actuarán de manera honesta, imparcial, transparente y profesional, con respeto a los derechos y los intereses de la clientela.

Toda información dirigida a su clientela, incluida la de carácter publicitario, deberá ser clara, suficiente, objetiva y no engañosa. Además, las entidades de crédito deberán en todo momento mantener adecuadamente informados a sus clientes, conforme a lo dispuesto en los apartados siguientes, las disposiciones de desarrollo y el resto de la normativa aplicable.

2. Sin perjuicio de la reglas de cálculo de la TAE establecidas en el anexo II y la Ficha Europea de Información Normalizada recogida en el Anexo I de la Ley 5/2019, de 15 de marzo, reguladora de los contratos de crédito inmobiliario, la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, con el fin de proteger los legítimos intereses de los clientes de servicios a productos bancarios, distintos de los de inversión, prestados por las entidades de crédito, y de los de préstamo objeto de dicha Ley, podrá dictar disposiciones relativas a:

a) La información precontractual que debe facilitarse a los clientes, la información y contenido de los contratos y las comunicaciones posteriores que permitan el seguimiento de los mismos, de modo que reflejen de forma explícita y con la máxima claridad los derechos y obligaciones de las partes, los riesgos derivados del servicio o producto para el cliente y las demás circunstancias necesarias para garantizar la transparencia de las condiciones más relevantes de los servicios o productos y permitir al cliente evaluar si estos se ajustan a sus necesidades y a su situación financiera. A tal efecto, los contratos de estos servicios o productos siempre se formalizarán por escrito o en formato electrónico o en otro soporte

duradero y la persona titular del Ministerio de Asuntos Económicos y Transformación Digital podrá, en particular, fijar las cláusulas que los contratos referentes a servicios o productos bancarios típicos habrán de tratar o prever de forma expresa.

b) La transparencia de las condiciones básicas de comercialización o contratación de los servicios o productos bancarios que ofrecen las entidades de crédito y, en su caso, el deber y la forma en que deben comunicar tales condiciones a su clientela o al Banco de España. Se podrán establecer, asimismo, condiciones básicas de los servicios o productos bancarios de debido cumplimiento para las entidades de crédito. En particular, solo podrán percibirse comisiones o repercutirse gastos por servicios solicitados en firme o aceptados expresamente por un cliente y siempre que respondan a servicios efectivamente prestados o gastos habidos que puedan acreditarse.

c) Los principios y criterios a los que debe sujetarse la actividad publicitaria de los servicios o productos bancarios, y las modalidades de control administrativo sobre la misma, con la finalidad de que esta resulte clara, suficiente, objetiva y no engañosa.

d) Las especialidades de la contratación de servicios o productos bancarios de forma electrónica o por otras vías de comunicación a distancia y la información que, al objeto de lo previsto en este artículo, debe figurar en las páginas electrónicas de las entidades de crédito.

e) El ámbito de aplicación de las normas dictadas al amparo de este artículo a cualesquiera contratos u operaciones de la naturaleza prevista en dichas normas, aun cuando la entidad que intervenga no tenga la condición de entidad de crédito.

f) La definición, el alcance y la aplicación de políticas, procedimientos y controles internos adecuados exigibles a las entidades de crédito para garantizar el debido cumplimiento de las obligaciones que la normativa de conducta y transparencia bancaria les impone, en particular, el desarrollo de lo establecido en el artículo 29.8.

3. En particular, en la comercialización de préstamos o créditos, la persona titular del Ministerio de Asuntos Económicos y Transformación Digital podrá dictar normas que favorezcan:

a) La adecuada atención a los ingresos de los clientes en relación con los compromisos que adquieran al recibir un préstamo.

b) La adecuada e independiente valoración de las garantías inmobiliarias que aseguren los préstamos de forma que se contemplen mecanismos que eviten las influencias indebidas de la propia entidad o de sus filiales en la valoración.

c) La consideración de diferentes escenarios de evolución de los tipos en los préstamos a interés variable, las posibilidades de cobertura frente a tales variaciones y todo ello teniendo además en cuenta el uso o no de índices oficiales de referencia.

d) La obtención y documentación apropiada de datos relevantes del solicitante.

e) La información precontractual y asistencia apropiadas para el cliente.

f) El respeto de las normas de protección de datos.

4. Sin perjuicio de la libertad contractual, el Ministerio de Asuntos Económicos y Transformación Digital podrá efectuar, por sí o a través del Banco de España, la publicación regular, con carácter oficial, de determinados índices o tipos de interés de referencia que puedan ser aplicados por las entidades de crédito a los préstamos a interés variable, especialmente en el caso de créditos o préstamos hipotecarios. Los citados índices o tipos de referencia deberán ser claros, accesibles, objetivos y verificables.

Los proveedores de estos índices para el cálculo de los tipos deudores y los prestamistas deberán conservar registros históricos de dichos índices.

5. Las disposiciones que en el ejercicio de sus competencias puedan dictar las Comunidades Autónomas sobre las materias contempladas en este artículo no podrán establecer un nivel de protección inferior al dispensado en las normas que apruebe la persona titular del Ministerio de Asuntos Económicos y Transformación Digital. Asimismo, podrán establecerse con carácter básico modelos normalizados de información que no podrán ser modificados por la normativa autonómica, en aras de la adecuada transparencia y homogeneidad de la información suministrada a los clientes de servicios o productos bancarios.

6. Las normas dictadas al amparo de lo previsto en este artículo serán consideradas normativa de ordenación y disciplina y su supervisión corresponderá al Banco de España.

[. . .]

TÍTULO III

Supervisión

CAPÍTULO I

Función supervisora

Artículo 50. *Función supervisora del Banco de España.*

1. El Banco de España es la autoridad responsable de la supervisión de las entidades de crédito y de las demás entidades previstas en el artículo 56, para garantizar el cumplimiento de la normativa de ordenación y disciplina. Para el ejercicio de esta función podrá desarrollar las actuaciones y ejercer las facultades previstas en esta Ley y cualesquiera otras que le atribuya el ordenamiento jurídico.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio de las competencias que el ordenamiento jurídico atribuya a otras instituciones u órganos administrativos.

2. En el ejercicio de su función supervisora y, en particular, para la elección de los distintos instrumentos de supervisión y sanción, el Banco de España podrá:

a) Recabar de las entidades y personas sujetas a su función supervisora, y a terceros a los que dichas entidades hayan subcontratado actividades o funciones operativas, la información necesaria para comprobar el cumplimiento de la normativa de ordenación y disciplina.

Con el fin de que el Banco de España pueda obtener dichas informaciones, o confirmar su veracidad, las entidades y personas mencionadas quedan obligadas a poner a disposición del Banco de España cuantos libros, registros y documentos considere precisos, incluidos los programas informáticos, ficheros y bases de datos, sea cuál sea su soporte físico o virtual.

A tales efectos, el acceso a las informaciones y datos requeridos por el Banco de España se encuentra amparado por el artículo 11.2.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

b) Requerir y comunicar a las entidades sujetas a su función supervisora, por medios electrónicos, las informaciones y medidas recogidas en la normativa de ordenación y disciplina. Las entidades referidas tendrán obligación de habilitar, en el plazo que se fije para ello, los medios técnicos requeridos por el Banco de España para la eficacia de sus sistemas de comunicación electrónica, en los términos que éste adopte al efecto.

c) Llevar a cabo todas las investigaciones necesarias en relación con cualquier entidad o persona de las contempladas en la letra a), cuando sea necesario para desempeñar su función supervisora. A estos efectos, podrá:

1.º Exigir la presentación de documentos.

2.º Examinar los libros y registros y obtener copias o extractos de los mismos.

3.º Solicitar y obtener explicaciones escritas o verbales de cualquier otra persona diferente de las previstas en la letra a) a fin de recabar información relacionada con el objeto de una investigación.

d) Realizar cuantas inspecciones sean necesarias en los establecimientos profesionales de las personas jurídicas contempladas en la letra a), y en cualquier otra entidad incluida en la supervisión consolidada.

3. Asimismo, en el ejercicio de su función supervisora, el Banco de España deberá:

a) Valorar, en la elección de las medidas que se vayan a adoptar, criterios como la gravedad de los hechos detectados, la eficacia de la propia función supervisora en términos

de la subsanación de los incumplimientos detectados o el comportamiento previo de la entidad.

b) Tomar en consideración la posible incidencia de sus decisiones en la estabilidad del sistema financiero de los demás Estados miembros de la Unión Europea afectados, particularmente en situaciones de urgencia, basándose en la información disponible en el momento de que se trate.

c) Tener en cuenta la convergencia de instrumentos y prácticas de supervisión en el ámbito de la Unión Europea.

4. En los términos previstos por el artículo 4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los órganos y organismos de cualquier Administración Pública, sin perjuicio del deber de secreto que les ampare conforme a la legislación vigente quedan sujetos al deber de colaborar con el Banco de España y están obligados a proporcionar, a requerimiento de éste, los datos e informaciones de que dispongan y puedan resultar necesarios para el ejercicio por parte de éste de la función supervisora.

5. Toda decisión que tome el Banco de España en el ejercicio de su potestad supervisora deberá ser debidamente motivada.

[. . .]

CAPÍTULO VI

Obligaciones de información y publicación

[. . .]

Artículo 83. *Deber de reserva de información.*

1. Las entidades y demás personas sujetas a la normativa de ordenación y disciplina de las entidades de crédito están obligadas a guardar reserva de las informaciones relativas a los saldos, posiciones, transacciones y demás operaciones de sus clientes sin que las mismas puedan ser comunicadas a terceros u objeto de divulgación.

2. Se exceptúan de este deber las informaciones respecto de las cuales el cliente o las leyes permitan su comunicación o divulgación a terceros o que, en su caso, les sean requeridas o hayan de remitir a las respectivas autoridades de supervisión o en el marco del cumplimiento de las obligaciones establecidas en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y la financiación del terrorismo. En este caso, la cesión de la información deberá ajustarse a lo dispuesto por el propio cliente o por las leyes.

3. Quedan asimismo exceptuadas del deber de reserva los intercambios de información entre entidades de crédito pertenecientes a un mismo grupo consolidable.

4. El incumplimiento de lo dispuesto en el presente artículo será considerado infracción grave y se sancionará en los términos y con arreglo al procedimiento previsto en el Título IV.

5. Lo previsto en este artículo se aplicará sin perjuicio de lo establecido en la normativa de protección de datos de carácter personal.

[. . .]

Artículo 115. *Publicidad de las sanciones.*

1. La imposición de las sanciones, con excepción de la de amonestación privada, se hará constar en los registros administrativos de entidades de crédito y altos cargos que correspondan.

2. Las sanciones de suspensión, separación y separación con inhabilitación, una vez sean ejecutivas, se harán constar, además, en el Registro Mercantil y, en su caso, en el Registro de Cooperativas.

3. El nombramiento de miembros del órgano de administración o de administradores provisionales a que se refiere el artículo 106, se hará constar también en los registros correspondientes.

4. Una vez que las sanciones impuestas a la entidad de crédito o a quienes ejerzan cargos de administración o dirección en la misma sean ejecutivas se comunicarán en la siguiente Junta o Asamblea General que se celebre.

5. Las sanciones y amonestaciones por infracciones muy graves y graves serán publicadas en el “Boletín Oficial del Estado” una vez que sean firmes en la vía administrativa. La publicación deberá incluir, por lo menos, información sobre el tipo y la naturaleza de la infracción y la identidad de las personas responsables de la misma.

6. En relación con lo previsto en el apartado anterior, excepcionalmente, el Banco de España podrá, o bien retrasar la publicación hasta el momento en que dejen de existir los motivos que justifiquen tal retraso, o bien publicar la sanción impuesta de forma anónima, cuando a su criterio se produzca alguna de las circunstancias siguientes:

a) Cuando la sanción se imponga a una persona física y, tras una evaluación previa, la publicación de los datos personales resulte ser desproporcionada.

b) Cuando la publicación pudiera poner en peligro la estabilidad de los mercados financieros o una investigación penal en curso.

c) Cuando la publicación pudiera causar un daño desproporcionado a las entidades o personas físicas implicadas, en la medida en que se pueda determinar el daño.

7. Las sanciones y amonestaciones por infracciones muy graves y graves deberán asimismo ser publicadas en la página web del Banco de España, en un plazo máximo de 15 días hábiles desde que la sanción o amonestación sea firme en vía administrativa, con el contenido de la información a la que se hace referencia en el apartado 5, pudiendo adoptarse las medidas contempladas en el apartado 6 en los supuestos en él previstos.

Cuando se interponga recurso en vía judicial contra la decisión de imponer una sanción o medida, el Banco de España también publicará de inmediato en su sitio web oficial esa información, así como toda información posterior relativa al resultado de ese recurso. Además, también se publicará toda decisión que anule o condone una decisión previa de imponer una sanción o medida.

El Banco de España mantendrá publicada toda la información a que se refieren los apartados anteriores en su sitio web oficial durante cinco años, como mínimo, tras su publicación.

[. . .]

§ 42

Ley 11/2022, de 28 de junio, General de Telecomunicaciones. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 155, de 29 de junio de 2022
Última modificación: 28 de junio de 2023
Referencia: BOE-A-2022-10757

[. . .]

TÍTULO III

Obligaciones de servicio público y derechos y obligaciones de carácter público en el suministro de redes y en la prestación de servicios de comunicaciones electrónicas

[. . .]

CAPÍTULO II

Derechos de los operadores y despliegue de redes públicas de comunicaciones electrónicas

Sección 1.ª Derechos de los operadores a la ocupación del dominio público, a ser beneficiarios en el procedimiento de expropiación forzosa y al establecimiento a su favor de servidumbres y de limitaciones a la propiedad

Artículo 44. *Derecho de ocupación de la propiedad privada.*

1. Los operadores tendrán derecho, en los términos de este capítulo, a la ocupación de la propiedad privada cuando resulte estrictamente necesario para la instalación, despliegue y explotación de la red en la medida prevista en el proyecto técnico presentado y siempre que no existan otras alternativas técnica o económicamente viables, ya sea a través de su expropiación forzosa o mediante la declaración de servidumbre forzosa de paso para la instalación, despliegue y explotación de infraestructura de redes públicas de comunicaciones electrónicas. En ambos casos tendrán la condición de beneficiarios en los expedientes que se tramiten, conforme a lo dispuesto en la legislación sobre expropiación forzosa.

Los operadores asumirán los costes a los que hubiera lugar por esta ocupación.

La ocupación de la propiedad privada se llevará a cabo tras la instrucción y resolución por el Ministerio de Asuntos Económicos y Transformación Digital del oportuno procedimiento, en que deberán cumplirse todos los trámites y respetarse todas las garantías establecidas a favor de los titulares afectados en la legislación de expropiación forzosa.

2. La aprobación por el órgano competente del Ministerio de Asuntos Económicos y Transformación Digital del proyecto técnico para la ocupación de propiedad privada llevará

implícita, en cada caso concreto, la declaración de utilidad pública y la necesidad de ocupación para la instalación de redes públicas de comunicaciones electrónicas, a efectos de lo previsto en la legislación de expropiación forzosa.

3. Con carácter previo a la aprobación del proyecto técnico, se recabará informe del órgano de la Comunidad Autónoma competente en materia de ordenación del territorio, que habrá de ser emitido en el plazo máximo de treinta días hábiles desde su solicitud. Si el proyecto afecta a un área geográfica relevante o pudiera tener afecciones ambientales, este plazo será ampliado hasta tres meses. Asimismo, se recabará informe de los Ayuntamientos afectados sobre compatibilidad del proyecto técnico con la ordenación urbanística vigente, que deberá ser emitido en el plazo de treinta días hábiles desde la recepción de la solicitud.

4. En las expropiaciones que se lleven a cabo para la instalación de redes públicas de comunicaciones electrónicas ligadas de manera específica al cumplimiento de obligaciones de servicio público se seguirá el procedimiento especial de urgencia establecido en la Ley de Expropiación Forzosa, cuando así se haga constar en la resolución del órgano competente del Ministerio de Asuntos Económicos y Transformación Digital que apruebe el oportuno proyecto técnico.

Artículo 45. *Derecho de ocupación del dominio público.*

Los operadores tendrán derecho, en los términos de este capítulo, a la ocupación del dominio público necesario para el establecimiento de la red pública de comunicaciones electrónicas de que se trate.

Los titulares del dominio público garantizarán el acceso de todos los operadores a dicho dominio en condiciones neutrales, objetivas, transparentes, equitativas y no discriminatorias, sin que en ningún caso pueda establecerse derecho preferente o exclusivo alguno de acceso u ocupación de dicho dominio público en beneficio de un operador determinado o de una red concreta de comunicaciones electrónicas. En particular, la ocupación o el derecho de uso de dominio público para la instalación o explotación de una red no podrá ser otorgado o asignado mediante procedimientos de licitación.

Se podrán celebrar acuerdos o convenios entre los operadores y los titulares o gestores del dominio público para facilitar el despliegue simultáneo de otros servicios, que deberán ser gratuitos para las Administraciones y los ciudadanos, vinculados a la mejora del medio ambiente, de la salud pública, de la seguridad pública y de la protección civil ante catástrofes naturales o para mejorar o facilitar la vertebración y cohesión territorial y urbana o contribuir a la sostenibilidad de la logística urbana.

La propuesta de acuerdo o convenio para la ocupación del dominio público deberá incluir un plan de despliegue e instalación con el contenido previsto en el artículo 49.9 de esta ley. Transcurrido el plazo máximo de tres meses desde su presentación, el acuerdo o convenio se entenderá aprobado si no hubiera pronunciamiento expreso en contra justificado adecuadamente.

Artículo 46. *Ubicación compartida y uso compartido de la propiedad pública o privada.*

1. Los operadores de redes públicas de comunicaciones electrónicas podrán celebrar de manera voluntaria acuerdos entre sí para determinar las condiciones para la ubicación o el uso compartido de sus elementos de red y recursos asociados, así como la utilización compartida del dominio público o la propiedad privada, con plena sujeción a la normativa de defensa de la competencia.

Las Administraciones públicas fomentarán la celebración de acuerdos voluntarios entre operadores para la ubicación compartida y el uso compartido de elementos de red y recursos asociados, así como la utilización compartida del dominio público o la propiedad privada, en particular con vistas al despliegue de elementos de las redes de comunicaciones electrónicas de alta y muy alta capacidad.

2. La ubicación compartida de elementos de red y recursos asociados y la utilización compartida del dominio público o la propiedad privada también podrá ser impuesta de manera obligatoria a los operadores que hayan ejercido el derecho a la ocupación de la propiedad pública o privada. A tal efecto, en los términos en que mediante real decreto se determine, el Ministerio de Asuntos Económicos y Transformación Digital, previo trámite de audiencia a los operadores afectados y de manera motivada, podrá imponer, con carácter

general o para casos concretos, la utilización compartida del dominio público o la propiedad privada en que se van a establecer las redes públicas de comunicaciones electrónicas o el uso compartido de los elementos de red y recursos asociados, determinando, en su caso, los criterios para compartir los gastos que produzca la ubicación o el uso compartido.

Cuando una Administración Pública competente considere que por razones de medio ambiente, salud pública, seguridad pública u ordenación urbana y territorial se justifica la imposición de la utilización compartida del dominio público o la propiedad privada, podrá instar de manera motivada al Ministerio de Asuntos Económicos y Transformación Digital el inicio del procedimiento establecido en el párrafo anterior. En estos casos, antes de que el Ministerio de Asuntos Económicos y Transformación Digital imponga la utilización compartida del dominio público o la propiedad privada, el citado departamento ministerial deberá realizar un trámite para que la Administración Pública competente que ha instado el procedimiento pueda efectuar alegaciones por un plazo de quince días hábiles.

3. Las medidas adoptadas de conformidad con el presente artículo deberán ser objetivas, transparentes, no discriminatorias y proporcionadas. Cuando proceda, estas medidas se aplicarán de forma coordinada con las Administraciones competentes correspondientes y con la Comisión Nacional de los Mercados y la Competencia.

Artículo 47. *Otras servidumbres y limitaciones a la propiedad.*

1. La protección del dominio público radioeléctrico tiene como finalidades su aprovechamiento óptimo, evitar su degradación y el mantenimiento de un adecuado nivel de calidad en el funcionamiento de los distintos servicios de radiocomunicaciones y aquellos otros que hacen uso del dominio público radioeléctrico.

El Ministerio de Asuntos Económicos y Transformación Digital podrá establecer las limitaciones a la propiedad y a la intensidad de campo eléctrico y las servidumbres que resulten necesarias para la protección radioeléctrica de determinadas instalaciones o para asegurar el adecuado funcionamiento de estaciones o instalaciones radioeléctricas utilizadas para la prestación de servicios públicos, por motivos de seguridad pública o cuando así sea necesario en virtud de acuerdos internacionales, en los términos de la disposición adicional segunda y las normas de desarrollo de esta ley.

2. Asimismo, el Ministerio de Asuntos Económicos y Transformación Digital podrá imponer límites a los derechos de uso del dominio público radioeléctrico para la protección de otros servicios o bienes jurídicamente protegidos prevalentes o de servicios públicos que puedan verse afectados por la utilización de dicho dominio público, en los términos que mediante real decreto se determinen. En la imposición de estos límites se debe efectuar un previo trámite de audiencia a los titulares de los derechos de uso del dominio público radioeléctrico que pueden verse afectados y se deberán respetar los principios de transparencia y publicidad.

Artículo 48. *Estudios geográficos.*

1. El Ministerio de Asuntos Económicos y Transformación Digital efectuará anualmente un estudio sobre el alcance y extensión de las redes de banda ancha, incluidas las redes de muy alta capacidad, con un nivel de desagregación local o incluso inferior.

El estudio geográfico incluirá información suficiente sobre la calidad del servicio y los parámetros de este último.

La información que no esté sujeta a confidencialidad comercial será accesible de conformidad con la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. El Ministerio de Asuntos Económicos y Transformación Digital informará a las empresas que proporcionen información en base a este artículo sobre el hecho de que la misma ha sido compartida con otras autoridades públicas, en su caso.

2. El Ministerio de Asuntos Económicos y Transformación Digital incluirá en el estudio geográfico una previsión sobre el alcance y extensión que van a tener las redes de banda ancha, incluidas las redes de muy alta capacidad, para un período determinado, con el grado de desagregación que estime oportuno.

Esta previsión será sometida a una consulta pública en la página web del Ministerio de Asuntos Económicos y Transformación Digital. En ella, a partir de una base de datos geográfica proporcionada por el Ministerio de Asuntos Económicos y Transformación Digital,

los operadores declararán cualquier intención de desplegar redes de banda ancha que ofrezca velocidades de descarga o transferencia de al menos 100 Mbps o redes de muy alta capacidad o de mejorar o extender significativamente sus redes hasta alcanzar una velocidad de descarga o transferencia de al menos 100 Mbps. Esta declaración de intenciones supone un compromiso en firme por parte del operador, de forma que su incumplimiento por causas imputables al operador que produzca un perjuicio al interés público en el diseño de planes nacionales de banda ancha, en la determinación de obligaciones de cobertura ligadas a los derechos de uso del espectro radioeléctrico o en la verificación de la disponibilidad de servicios en el marco de la obligación de servicio universal, o bien un perjuicio a otro operador, podrá ser sancionada en los términos previstos en el título VIII.

A la vista de las aportaciones efectuadas en la consulta pública, de las declaraciones de intenciones efectuadas y de otra información de que pueda disponer, el Ministerio de Asuntos Económicos y Transformación Digital elaborará y publicará una previsión definitiva sobre el alcance y extensión que van a tener las redes de banda ancha, incluidas las redes de muy alta capacidad, para un período determinado. Esta previsión incluirá toda la información pertinente, en particular, información del despliegue planeado de redes de muy alta capacidad y mejoras o extensiones de redes con una velocidad de descarga o transferencia de al menos 100 Mbps.

3. A efectos de la elaboración de estos estudios geográficos, el Ministerio de Asuntos Económicos y Transformación Digital podrá solicitar la información necesaria y ajustada a este fin, en los términos indicados en el artículo 9, a las personas físicas o jurídicas que suministren redes o presten servicios de comunicaciones electrónicas, así como a aquellos otros agentes que intervengan en este mercado o en mercados y sectores estrechamente relacionados, con el grado de desagregación oportuno.

El Ministerio de Asuntos Económicos y Transformación Digital también solicitará información para la elaboración de estos estudios geográficos al resto de Administraciones públicas, en particular, a las Comunidades Autónomas, Diputaciones provinciales y Ayuntamientos.

4. La información contenida en los estudios geográficos servirá de base para la elaboración de los planes nacionales de banda ancha o de conectividad digital, que priorizarán la cobertura de los núcleos de población más pequeños y del entorno rural, para el diseño de ayudas públicas para el despliegue de redes públicas de comunicaciones electrónicas, para la aplicación de la normativa sobre ayudas estatales, para la determinación de obligaciones de cobertura ligadas a los derechos de uso del espectro radioeléctrico y la verificación de la disponibilidad de servicios en el marco de la obligación de servicio universal.

La Comisión Nacional de los Mercados y la Competencia y otras Administraciones públicas también podrán basarse en la información que proporcionen los estudios geográficos para el ejercicio de sus funciones. A tal efecto, podrán solicitar al Ministerio de Asuntos Económicos y Transformación Digital la información oportuna, priorizando el acceso y tratamiento de dicha información por medios electrónicos. El Ministerio de Asuntos Económicos y Transformación Digital y la Comisión Nacional de los Mercados y la Competencia colaborarán en la determinación y desglose de la información a obtener para confeccionar los estudios geográficos, a efectos de que puedan ejercer con mayor eficacia y eficiencia sus funciones.

[. . .]

CAPÍTULO III

Salvaguardia de derechos fundamentales, secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas

Artículo 56. *Salvaguardia de derechos fundamentales.*

1. Las medidas que se adopten en relación al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas

respetarán los derechos y libertades fundamentales, como queda garantizado en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, en la Carta de Derechos Fundamentales de la Unión Europea, en los principios generales del Derecho comunitario y en la Constitución Española.

2. Cualquiera de esas medidas relativas al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas, que sea susceptible de restringir esos derechos y libertades fundamentales solo podrá imponerse si es adecuada, necesaria y proporcionada en una sociedad democrática, y su aplicación está sujeta a las salvaguardias de procedimiento apropiadas de conformidad con las normas mencionadas en el apartado anterior. Por tanto, dichas medidas solo podrán ser adoptadas respetando debidamente el principio de presunción de inocencia, el derecho a la vida privada e intimidad, el derecho a la libertad de expresión e información y el derecho a la tutela judicial efectiva, a través de un procedimiento previo, justo e imparcial, que incluirá el derecho de los interesados a ser oídos, sin perjuicio de que concurran las condiciones y los requisitos procedimentales adecuados en los casos de urgencia debidamente justificados, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales y la Carta de los Derechos Fundamentales de la Unión Europea.

Artículo 57. *Principio de no discriminación.*

Los operadores que instalen o exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público no aplicarán a los usuarios finales ningún requisito diferente ni condiciones generales de acceso o uso de redes o servicios ni de utilización de los mismos por motivos relacionados con la nacionalidad, el lugar de residencia o el lugar de establecimiento del usuario final, a menos que dicho trato diferente se justifique de forma objetiva.

Artículo 58. *Secreto de las comunicaciones.*

1. Los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones interpersonales basados en numeración disponibles al público o servicios de acceso a internet están obligados a realizar las interceptaciones que se autoricen judicialmente de acuerdo con lo establecido en el capítulo V del título VIII del libro II de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, éste podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas disponibles al público distintas de las comunicaciones interpersonales independientes de la numeración, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la

información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

Los sujetos obligados proporcionarán, cuando técnicamente sea posible, los identificadores permanentes que sean necesarios para la atribución de un servicio a un usuario determinado de forma inequívoca, así como los identificadores del dispositivo empleado para la comunicación.

Si en una comunicación electrónica se asignaran identidades de carácter temporal al usuario, el sujeto obligado implementará, cuando técnicamente sea posible, las medidas de correlación necesarias para que en la información de la interceptación se faciliten las identidades permanentes que permitan la identificación inequívoca del usuario asignado, así como del dispositivo empleado en la comunicación.

b) identidad o identidades de las otras partes involucradas en la comunicación electrónica;

c) servicios básicos utilizados;

d) servicios suplementarios utilizados;

e) dirección de la comunicación;

f) indicación de respuesta;

g) causa de finalización;

h) marcas temporales;

i) información de localización;

j) información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) identificación de la persona física o jurídica;

b) domicilio en el que el operador realiza las notificaciones;

y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado);

d) número de identificación del terminal;

e) número de cuenta asignada por el proveedor de servicios internet;

f) dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

8. Los sujetos obligados deberán facilitar al agente facultado, de entre los datos previstos en los apartados 5, 6 y 7 de este artículo, sólo aquéllos que estén incluidos en la orden de interceptación legal.

9. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida

de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de identidad de extranjero o pasaporte, en el caso de personas físicas, o denominación y número de identificación fiscal en el caso de personas jurídicas.

10. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que se establezcan por el Ministerio de Asuntos Económicos y Transformación Digital.

11. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.

Artículo 59. *Interceptación de las comunicaciones electrónicas por los servicios técnicos.*

1. Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico o para la localización de interferencias perjudiciales sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:

a) la administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma tal que se reduzca al mínimo el riesgo de afectar a los contenidos de las comunicaciones;

b) cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan deberán ser custodiados hasta la finalización, en su caso, del expediente sancionador que hubiera lugar o, en otro caso, destruidos inmediatamente. En ninguna circunstancia podrán ser objeto de divulgación.

2. Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de comunicaciones electrónicas.

3. Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el artículo 85.

Artículo 60. *Protección de los datos de carácter personal.*

1. Los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en el suministro de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal. Dichas medidas incluirán, como mínimo:

a) la garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley;

b) la protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos;

c) la garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

La Agencia Española de Protección de Datos, en el ejercicio de su competencia de garantía de la seguridad en el tratamiento de datos de carácter personal, podrá examinar las medidas adoptadas por los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público y podrá formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas.

2. En caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de comunicaciones electrónicas, el operador que suministre dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

3. En caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos. Si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el operador notificará también la violación al abonado o particular sin dilaciones indebidas.

La notificación de una violación de los datos personales a un abonado o particular afectado no será necesaria si el operador ha probado a satisfacción de la Agencia Española de Protección de Datos que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características podrían ser aquellas que convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.

Sin perjuicio de la obligación del operador de informar a los abonados o particulares afectados, si el operador no ha notificado ya al abonado o al particular la violación de los datos personales, la Agencia Española de Protección de Datos podrá exigirle que lo haga, una vez evaluados los posibles efectos adversos de la violación.

En la notificación al abonado o al particular se describirá al menos la naturaleza de la violación de los datos personales y los puntos de contacto donde puede obtenerse más información y se recomendarán medidas para atenuar los posibles efectos adversos de dicha violación. En la notificación a la Agencia Española de Protección de Datos se describirán además las consecuencias de la violación y las medidas propuestas o adoptadas por el operador respecto a la violación de los datos personales.

Los operadores deberán llevar un inventario de las violaciones de los datos personales, incluidos los hechos relacionados con tales infracciones, sus efectos y las medidas adoptadas al respecto, que resulte suficiente para permitir a la Agencia Española de Protección de Datos verificar el cumplimiento de las obligaciones de notificación reguladas en este apartado. Mediante real decreto podrá establecerse el formato y contenido del inventario.

A los efectos establecidos en este artículo, se entenderá como violación de los datos personales la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público.

La Agencia Española de Protección de Datos podrá adoptar directrices y, en caso necesario, dictar instrucciones sobre las circunstancias en que se requiere que el operador notifique la violación de los datos personales, sobre el formato que debe adoptar dicha notificación y sobre la manera de llevarla a cabo, con pleno respeto a las disposiciones que en su caso sean adoptadas en esta materia por la Comisión Europea.

4. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y su normativa de desarrollo.

Artículo 61. *Conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.*

La conservación y cesión de los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Artículo 62. *Cifrado en las redes y servicios de comunicaciones electrónicas.*

1. Cualquier tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado.

2. El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, en casos justificados de protección de los intereses esenciales de seguridad del Estado y la seguridad pública, y para permitir la investigación, la detección y el enjuiciamiento de delitos, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente.

3. Toda información obtenida por parte de la Administración General del Estado o cualquier organismo público a través de los preceptos incluidos en el apartado 2 de este artículo deberá ser tratada con la máxima confidencialidad y destruida una vez que se resuelva la amenaza para la seguridad del Estado y la seguridad pública o se haya dictado sentencia firme sobre el delito en cuestión.

Artículo 63. *Integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas.*

1. Los operadores de redes públicas de comunicaciones electrónicas y de servicios de comunicaciones electrónicas disponibles al público, gestionarán adecuadamente los riesgos de seguridad que puedan afectar a sus redes y servicios a fin de garantizar un adecuado nivel de seguridad y evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en otras redes y servicios, para lo cual deberán adoptar las medidas técnicas y organizativas adecuadas, que deberán ser proporcionadas y en línea con el estado de la técnica, pudiendo incluir el cifrado.

2. Asimismo, los operadores de redes públicas de comunicaciones electrónicas garantizarán la integridad de las mismas a fin de asegurar la continuidad en la prestación de los servicios que utilizan dichas redes.

3. Los operadores que suministren redes públicas o presten servicios de comunicaciones electrónicas disponibles al público notificarán al Ministerio de Asuntos Económicos y Transformación Digital los incidentes de seguridad que hayan tenido un impacto significativo en el suministro de las redes o los servicios.

Con el fin de determinar la importancia del impacto de un incidente de seguridad se tendrán en cuenta, en particular, los parámetros siguientes, cuando se disponga de ellos:

a) el número de usuarios afectados por el incidente de seguridad;
b) la duración del incidente de seguridad;
c) el área geográfica afectada por el incidente de seguridad;
d) la medida en que se ha visto afectado el funcionamiento de la red o del servicio;
e) el alcance del impacto sobre las actividades económicas y sociales.

Cuando proceda, el Ministerio informará a las autoridades nacionales competentes de otros Estados miembros y a la Agencia Europea de Seguridad en las Redes y la Información (ENISA). Asimismo, podrá informar al público o exigir a los operadores que lo hagan, en caso de estimar que la divulgación del incidente de seguridad reviste interés público. Una

vez al año, el Ministerio presentará a la Comisión y a la ENISA un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de conformidad con este apartado.

Del mismo modo, el Ministerio comunicará a la Secretaría de Estado de Seguridad del Ministerio del Interior aquellos incidentes que afectando a los operadores estratégicos nacionales sean de interés para la mejora de la protección de infraestructuras críticas, en el marco de la Ley 8/2011, de 28 de abril, reguladora de las mismas. También el Ministerio comunicará a la Comisión Nacional de los Mercados y la Competencia los incidentes de seguridad a que se refiere este apartado que afecten o puedan afectar a las obligaciones específicas impuestas por dicha Comisión en los mercados de referencia.

4. En caso de que exista una amenaza particular y significativa de incidente de seguridad en las redes públicas de comunicaciones electrónicas o en los servicios de comunicaciones electrónicas disponibles para el público, los operadores deberán informar a sus usuarios que pudieran verse afectados por dicha amenaza sobre las posibles medidas de protección o soluciones que pueden adoptar los usuarios. Cuando proceda, los operadores también informarán a sus usuarios sobre la propia amenaza.

5. El Ministerio de Asuntos Económicos y Transformación Digital establecerá los mecanismos para supervisar el cumplimiento de las obligaciones anteriores y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para los operadores, incluidas las relativas a las medidas necesarias adicionales a las identificadas por los operadores para solventar incidentes de seguridad, o impedir que ocurran cuando se haya observado una amenaza significativa, e incumplimientos de las fechas límite de aplicación. Entre las medidas relativas a la integridad y seguridad de redes y servicios de comunicaciones electrónicas que se puedan exigir a los operadores, podrá imponer:

a) la obligación de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad;

b) la obligación de someterse a una auditoría de seguridad realizada por un organismo independiente o por una autoridad competente, y de poner el resultado a disposición del Ministerio de Asuntos Económicos y Transformación Digital. El coste de la auditoría será sufragado por el operador.

6. En particular, los operadores garantizarán la mayor disponibilidad posible de los servicios de comunicaciones vocales y de acceso a internet a través de las redes públicas de comunicaciones electrónicas en caso de fallo catastrófico de la red o en casos de fuerza mayor, y adoptarán todas las medidas necesarias para garantizar el acceso sin interrupciones a los servicios de emergencia y la transmisión ininterrumpida de las alertas públicas.

7. El presente artículo se entiende sin perjuicio de lo establecido en el artículo 4.6.

8. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo.

[. . .]

§ 43

Ley 5/2014, de 4 de abril, de Seguridad Privada. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 83, de 5 de abril de 2014
Última modificación: 27 de mayo de 2021
Referencia: BOE-A-2014-3649

[. . .]

TÍTULO I

Coordinación

[. . .]

Artículo 15. *Acceso a la información por las Fuerzas y Cuerpos de Seguridad.*

1. Se autorizan las cesiones de datos que se consideren necesarias para contribuir a la salvaguarda de la seguridad ciudadana, así como el acceso por parte de las Fuerzas y Cuerpos de Seguridad a los sistemas instalados por las empresas de seguridad privada que permitan la comprobación de las informaciones en tiempo real cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

2. El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de esta ley se someterán a lo dispuesto en la normativa de protección de datos de carácter personal.

3. La comunicación de buena fe de información a las Fuerzas y Cuerpos de Seguridad por las entidades y el personal de seguridad privada no constituirá vulneración de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa, cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

[. . .]

TÍTULO IV

Servicios y medidas de seguridad

[. . .]

CAPÍTULO II

Servicios de las empresas de seguridad privada

[. . .]

Artículo 42. *Servicios de videovigilancia.*

1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.

Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales.

No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada.

2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular.

3. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas, no requerirán autorización administrativa para su instalación, empleo o utilización.

4. Las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales.

5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

6. En lo no previsto en la presente ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad.

[. . .]

CAPÍTULO III

Servicios de los despachos de detectives privados

Artículo 48. *Servicios de investigación privada.*

1. Los servicios de investigación privada, a cargo de detectives privados, consistirán en la realización de las averiguaciones que resulten necesarias para la obtención y aportación, por cuenta de terceros legitimados, de información y pruebas sobre conductas o hechos privados relacionados con los siguientes aspectos:

a) Los relativos al ámbito económico, laboral, mercantil, financiero y, en general, a la vida personal, familiar o social, exceptuada la que se desarrolle en los domicilios o lugares reservados.

b) La obtención de información tendente a garantizar el normal desarrollo de las actividades que tengan lugar en ferias, hoteles, exposiciones, espectáculos, certámenes,

convenciones, grandes superficies comerciales, locales públicos de gran concurrencia o ámbitos análogos.

c) La realización de averiguaciones y la obtención de información y pruebas relativas a delitos sólo perseguibles a instancia de parte por encargo de los sujetos legitimados en el proceso penal.

2. La aceptación del encargo de estos servicios por los despachos de detectives privados requerirá, en todo caso, la acreditación, por el solicitante de los mismos, del interés legítimo alegado, de lo que se dejará constancia en el expediente de contratación e investigación que se abra.

3. En ningún caso se podrá investigar la vida íntima de las personas que transcurra en sus domicilios u otros lugares reservados, ni podrán utilizarse en este tipo de servicios medios personales, materiales o técnicos de tal forma que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones o a la protección de datos.

4. En la prestación de los servicios de investigación, los detectives privados no podrán utilizar o hacer uso de medios, vehículos o distintivos que puedan confundirse con los de las Fuerzas y Cuerpos de Seguridad.

5. En todo caso, los despachos de detectives y los detectives privados encargados de las investigaciones velarán por los derechos de sus clientes con respeto a los de los sujetos investigados.

6. Los servicios de investigación privada se ejecutarán con respeto a los principios de razonabilidad, necesidad, idoneidad y proporcionalidad.

Artículo 49. *Informes de investigación.*

1. Por cada servicio que les sea contratado, los despachos o los detectives privados encargados del asunto deberán elaborar un único informe en el que reflejarán el número de registro asignado al servicio, los datos de la persona que encarga y contrata el servicio, el objeto de la contratación, los medios, los resultados, los detectives intervinientes y las actuaciones realizadas, en las condiciones y plazos que reglamentariamente se establezcan.

2. En el informe de investigación únicamente se hará constar información directamente relacionada con el objeto y finalidad de la investigación contratada, sin incluir en él referencias, informaciones o datos que hayan podido averiguarse relativos al cliente o al sujeto investigado, en particular los de carácter personal especialmente protegidos, que no resulten necesarios o que no guarden directa relación con dicho objeto y finalidad ni con el interés legítimo alegado para la contratación.

3. Dicho informe estará a disposición del cliente, a quien se entregará, en su caso, al finalizar el servicio, así como a disposición de las autoridades policiales competentes para la inspección, en los términos previstos en el artículo 54.5.

4. Los informes de investigación deberán conservarse archivados, al menos, durante tres años, sin perjuicio de lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Las imágenes y los sonidos grabados durante las investigaciones se destruirán tres años después de su finalización, salvo que estén relacionadas con un procedimiento judicial, una investigación policial o un procedimiento sancionador. En todo caso, el tratamiento de dichas imágenes y sonidos deberá observar lo establecido en la normativa sobre protección de datos de carácter personal, especialmente sobre el bloqueo de datos previsto en la misma.

5. Las investigaciones privadas tendrán carácter reservado y los datos obtenidos a través de las mismas solo se podrán poner a disposición del cliente o, en su caso, de los órganos judiciales y policiales, en este último supuesto únicamente para una investigación policial o para un procedimiento sancionador, conforme a lo dispuesto en el artículo 25.

[. . .]

TÍTULO VI

Régimen sancionador

CAPÍTULO I

Infracciones

[. . .]

Artículo 57. *Infracciones de las empresas que desarrollen actividades de seguridad privada, de sus representantes legales, de los despachos de detectives privados y de las centrales de alarma de uso propio.*

Las empresas que desarrollen actividades de seguridad privada, sus representantes legales, los despachos de detectives privados y las centrales de alarma de uso propio, podrán incurrir en las siguientes infracciones:

1. Infracciones muy graves:

a) La prestación de servicios de seguridad privada a terceros careciendo de autorización o, en su caso, sin haber presentado la declaración responsable prevista en el artículo 18.1 y 2 para la prestación de los servicios de que se trate.

b) La contratación o utilización, en servicios de seguridad privada, de personas que carezcan de la habilitación o acreditación correspondiente.

c) La realización de actividades prohibidas en el artículo 8.4, sobre reuniones o manifestaciones, conflictos políticos o laborales, control de opiniones o su expresión, o la información a terceras personas sobre bienes de cuya seguridad o investigación hubieran sido encargados, o cualquier otra forma de quebrantamiento del deber de reserva, cuando no sean constitutivas de delito y salvo que sean constitutivas de infracción a la normativa sobre protección de datos de carácter personal.

d) La instalación o utilización de medios materiales o técnicos no homologados cuando la homologación sea preceptiva y sean susceptibles de causar grave daño a las personas o a los intereses generales.

e) La negativa a facilitar, cuando proceda, la información contenida en los contratos de seguridad privada, en los libros-registro o el acceso a los informes de investigación privada.

f) El incumplimiento de las previsiones normativas sobre adquisición y uso de armas, así como sobre disponibilidad de armeros y custodia de aquéllas, particularmente la tenencia de armas por el personal a su servicio fuera de los casos permitidos por esta ley, o la contratación de instructores de tiro que carezcan de la oportuna habilitación.

g) La prestación de servicios de seguridad privada con armas de fuego fuera de lo dispuesto en esta ley.

h) La negativa a prestar auxilio o colaboración a las Fuerzas y Cuerpos de Seguridad en la investigación y persecución de actos delictivos; en el descubrimiento y detención de los delincuentes; o en la realización de las funciones inspectoras o de control que les correspondan.

i) El incumplimiento de la obligación que impone a los representantes legales el artículo 22.3.

j) La ausencia de las medidas de seguridad obligatorias, por parte de las empresas de seguridad privada y los despachos de detectives, en sus sedes, delegaciones y sucursales.

k) El incumplimiento de las condiciones de prestación de servicios establecidos por la autoridad competente en relación con el ejercicio del derecho de huelga en servicios esenciales, o en los que el servicio de seguridad se haya impuesto obligatoriamente, en los supuestos a que se refiere el artículo 8.6.

l) El incumplimiento de los requisitos que impone a las empresas de seguridad el artículo 19. 1, 2 y 3, y el artículo 35.2.

m) El incumplimiento de los requisitos que impone a los despachos de detectives el artículo 24. 1 y 2.

n) La falta de transmisión a las Fuerzas y Cuerpos de Seguridad competentes de las alarmas reales que se registren en las centrales receptoras de alarmas privadas, incluidas

las de uso propio, así como el retraso en la transmisión de las mismas, cuando estas conductas no estén justificadas.

ñ) La prestación de servicios compatibles contemplados en el artículo 6.2, empleando personal no habilitado que utilice armas o medios de defensa reservados al personal de seguridad privada.

o) La realización de investigaciones privadas a favor de solicitantes en los que no concurra un interés legítimo en el asunto.

p) La prestación de servicios de seguridad privada sin formalizar los correspondientes contratos.

q) El empleo o utilización, en servicios de seguridad privada, de medidas o de medios personales, materiales o técnicos de forma que se atente contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones, siempre que no constituyan delito.

r) La falta de comunicación por parte de empresas de seguridad informática de las incidencias relativas al sistema de cuya protección sean responsables cuando sea preceptivo.

s) La comisión de una tercera infracción grave o de una grave y otra muy grave en el período de dos años, habiendo sido sancionado por las anteriores.

t) La prestación de actividades ajenas a las de seguridad privada, excepto las compatibles previstas en el artículo 6 de la presente ley.

2. Infracciones graves:

a) La instalación o utilización de medios materiales o técnicos no homologados, cuando la homologación sea preceptiva.

b) La prestación de servicios de seguridad privada con vehículos, uniformes, distintivos, armas o medios de defensa que no reúnan las características reglamentarias.

c) La prestación de servicios de seguridad privada careciendo de los requisitos específicos de autorización o presentación de declaración responsable para la realización de dicho tipo de servicios. Esta infracción también será aplicable cuando tales servicios se lleven a cabo fuera del lugar o del ámbito territorial para el que estén autorizados o se haya presentado la declaración responsable, o careciendo de la autorización previa o de dicha declaración cuando éstas sean preceptivas, o cuando se realicen en condiciones distintas a las expresamente previstas en la autorización del servicio.

d) La retención de la documentación profesional del personal de seguridad privada, o de la acreditación del personal acreditado.

e) La prestación de servicios de seguridad privada sin comunicar correctamente los correspondientes contratos al Ministerio del Interior o al órgano autonómico competente, o en los casos en que la comunicación se haya producido con posterioridad al inicio del servicio.

f) La prestación de servicios de seguridad privada sin cumplir lo estipulado en el correspondiente contrato.

g) La falta de sustitución ante el abandono o la omisión injustificados del servicio por parte del personal de seguridad privada, dentro de la jornada laboral establecida.

h) La utilización, en el desempeño de funciones de seguridad privada, de personal de seguridad privada, con una antigüedad mínima de un año en la empresa, que no haya realizado los correspondientes cursos de actualización o especialización, no los haya superado, o no los haya realizado con la periodicidad que reglamentariamente se determine.

i) La falta de presentación al Ministerio del Interior o al órgano autonómico competente del certificado acreditativo de la vigencia del contrato de seguro, aval o seguro de caución en los términos establecidos en el artículo 19.1.e) y f) y 24.2.e) y f), así como la no presentación del informe de actividades y el resumen de la cuenta anual a los que se refiere el artículo 21.1.e), o la no presentación de la memoria a la que se refiere el artículo 25.1.i)

j) La comunicación de una o más falsas alarmas por negligencia, deficiente funcionamiento o falta de verificación previa.

k) La apertura de delegaciones o sucursales sin obtener la autorización necesaria o sin haber presentado la declaración responsable ante el órgano competente, cuando sea preceptivo.

l) La falta de comunicación al Ministerio del Interior o, en su caso, al órgano autonómico competente, de las altas y bajas del personal de seguridad privada, así como de los cambios que se produzcan en sus representantes legales y toda variación en la composición personal de los órganos de administración, gestión, representación y dirección.

m) La prestación de servicio por parte del personal de seguridad privada sin la debida uniformidad o sin los medios que reglamentariamente sean exigibles.

n) La no realización de las revisiones anuales obligatorias de los sistemas o medidas de seguridad cuyo mantenimiento tuvieren contratado.

ñ) La carencia o falta de cumplimentación de cualquiera de los libros-registro obligatorios.

o) La falta de comunicación al Ministerio del Interior o, en su caso, al órgano autonómico competente de todo cambio relativo a su personalidad o forma jurídica, denominación, número de identificación fiscal o domicilio.

p) La falta de mantenimiento, en todo momento, de los requisitos establecidos para los representantes legales en el artículo 22.2.

q) El deficiente funcionamiento, por parte de las empresas de seguridad privada y despachos de detectives, en sus sedes, delegaciones o sucursales, de las medidas de seguridad obligatorias, así como el incumplimiento de las revisiones obligatorias de las mismas.

r) La prestación de servicios compatibles contemplados en el artículo 6.2 empleando personal no habilitado que utilice distintivos, uniformes o medios que puedan confundirse con los del personal de seguridad privada.

s) El incumplimiento de los requisitos impuestos a las empresas de seguridad informática.

t) La prestación de servicios incumpliendo lo dispuesto en el artículo 19.4.

u) La actuación de vigilantes de seguridad en el exterior de las instalaciones, inmuebles o propiedades de cuya vigilancia o protección estuvieran encargadas las empresas de seguridad privada con motivo de la prestación de servicios de tal naturaleza, fuera de los supuestos legalmente previstos.

v) No depositar la documentación profesional sobre contratos, informes de investigación y libros-registros en las dependencias del Cuerpo Nacional de Policía o, en su caso, del cuerpo de policía autonómico competente, en caso de cierre del despacho de detectives privados.

w) La comisión de una tercera infracción leve o de una grave y otra leve, en el período de dos años, habiendo recaído sanción por las anteriores.

x) La publicidad de servicios de seguridad privada por parte de personas, físicas o jurídicas, carentes de la correspondiente autorización o sin haber presentado declaración responsable.

y) La prestación de servicios de seguridad privada en condiciones distintas a las previstas en las comunicaciones de los correspondientes contratos.

3. Infracciones leves:

a) El incumplimiento de la periodicidad de las revisiones obligatorias de los sistemas o medidas de seguridad cuyo mantenimiento tuvieren contratado.

b) La utilización en los servicios de seguridad privada de vehículos, uniformes o distintivos con apariencia o semejanza a los de las Fuerzas y Cuerpos de Seguridad o de las Fuerzas Armadas.

c) La falta de diligencia en la cumplimentación de los libros-registro obligatorios.

d) En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por esta ley, siempre que no constituya infracción grave o muy grave.

Artículo 58. *Infracciones del personal que desempeñe funciones de seguridad privada.*

El personal que desempeñe funciones de seguridad privada, así como los ingenieros, técnicos, operadores de seguridad y profesores acreditados, podrán incurrir en las siguientes infracciones:

1. Infracciones muy graves:

a) El ejercicio de funciones de seguridad privada para terceros careciendo de la habilitación o acreditación necesaria.

b) El incumplimiento de las previsiones contenidas en esta ley sobre tenencia de armas de fuego fuera del servicio y sobre su utilización.

c) La falta de reserva debida sobre los hechos que conozcan en el ejercicio de sus funciones o la utilización de medios materiales o técnicos de tal forma que atenten contra el derecho al honor, a la intimidad personal o familiar, a la propia imagen o al secreto de las comunicaciones cuando no constituyan delito.

d) La negativa a prestar auxilio o colaboración a las Fuerzas y Cuerpos de Seguridad, cuando sea procedente, en la investigación y persecución de actos delictivos; en el descubrimiento y detención de los delincuentes; o en la realización de las funciones inspectoras o de control que les correspondan.

e) La negativa a identificarse profesionalmente, en el ejercicio de sus respectivas funciones, ante la Autoridad o sus agentes, cuando fueren requeridos para ello.

f) La realización de investigaciones sobre delitos perseguibles de oficio o la falta de denuncia a la autoridad competente de los delitos que conozcan los detectives privados en el ejercicio de sus funciones.

g) La realización de actividades prohibidas en el artículo 8.4 sobre reuniones o manifestaciones, conflictos políticos y laborales, control de opiniones o su expresión, o la información a terceras personas sobre bienes de cuya seguridad estén encargados, en el caso de que no sean constitutivas de delito; salvo que sean constitutivas infracción a la normativa sobre protección de datos de carácter personal.

h) El ejercicio abusivo de sus funciones en relación con los ciudadanos.

i) La realización, orden o tolerancia, en el ejercicio de su actuación profesional, de prácticas abusivas, arbitrarias o discriminatorias, incluido el acoso, que entrañen violencia física o moral, cuando no constituyan delito.

j) El abandono o la omisión injustificados del servicio por parte del personal de seguridad privada, dentro de la jornada laboral establecida.

k) La elaboración de proyectos o ejecución de instalaciones o mantenimientos de sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, sin disponer de la acreditación correspondiente expedida por el Ministerio del Interior.

l) La no realización del informe de investigación que preceptivamente deben elaborar los detectives privados o su no entrega al contratante del servicio, o la elaboración de informes paralelos.

m) El ejercicio de funciones de seguridad privada por parte del personal a que se refiere el artículo 28.3 y 4.

n) La comisión de una tercera infracción grave o de una grave y otra muy grave en el período de dos años, habiendo sido sancionado por las anteriores.

2. Infracciones graves:

a) La realización de funciones de seguridad privada que excedan de la habilitación obtenida.

b) El ejercicio de funciones de seguridad privada por personal habilitado, no integrado en empresas de seguridad privada, o en la plantilla de la empresa, cuando resulte preceptivo conforme a lo dispuesto en el artículo 38.5, o al margen de los despachos de detectives.

c) La falta de respeto al honor o a la dignidad de las personas.

d) El ejercicio del derecho a la huelga al margen de lo dispuesto al respecto para los servicios que resulten o se declaren esenciales por la autoridad pública competente, o en los que el servicio de seguridad se haya impuesto obligatoriamente, en los supuestos a que se refiere el artículo 8.6.

e) La no identificación profesional, en el ejercicio de sus respectivas funciones, cuando fueren requeridos para ello por los ciudadanos.

f) La retención de la documentación personal en contra de lo previsto en el artículo 32.1.b).

g) La falta de diligencia en el cumplimiento de las respectivas funciones por parte del personal habilitado o acreditado.

h) La identificación profesional haciendo uso de documentos o distintivos diferentes a los dispuestos legalmente para ello o acompañando éstos con emblemas o distintivos de apariencia semejante a los de las Fuerzas y Cuerpos de Seguridad o de las Fuerzas Armadas.

i) La negativa a realizar los cursos de formación permanente a los que vienen obligados.

j) La elaboración de proyectos o ejecución de instalaciones o mantenimientos de sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, no ajustados a las normas técnicas reglamentariamente establecidas.

k) La omisión, total o parcial, de los datos que obligatoriamente debe contener el informe de investigación que deben elaborar los detectives privados.

l) El ejercicio de funciones de seguridad privada incompatibles entre sí, por parte de personal habilitado para ellas.

m) La comisión de una tercera infracción leve o de una grave y otra leve, en el período de dos años, habiendo recaído sanción por las anteriores.

n) La validación provisional de sistemas o medidas de seguridad que no se adecuen a la normativa de seguridad privada.

3. Infracciones leves:

a) La actuación sin la debida uniformidad o medios, que reglamentariamente sean exigibles, o sin portar los distintivos o la documentación profesional, así como la correspondiente al arma de fuego utilizada en la prestación del servicio encomendado.

b) El trato incorrecto o desconsiderado con los ciudadanos.

c) La no cumplimentación, total o parcial, por parte de los técnicos acreditados, del documento justificativo de las revisiones obligatorias de los sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia.

d) En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por esta ley, siempre que no constituya infracción grave o muy grave.

[. . .]

§ 44

Ley 26/2013, de 27 de diciembre, de cajas de ahorros y fundaciones bancarias. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 311, de 28 de diciembre de 2013
Última modificación: 7 de mayo de 2020
Referencia: BOE-A-2013-13723

[. . .]

TÍTULO II

De las fundaciones bancarias

[. . .]

CAPÍTULO V

Régimen de control

[. . .]

Artículo 46. *Funciones del Banco de España.*

1. Sin perjuicio de lo previsto en el título VI de la Ley 26/1988, de 29 de julio, sobre Disciplina e Intervención de las Entidades de Crédito, corresponderá al Banco de España el control del cumplimiento de las normas contenidas en el capítulo IV de esta Ley desde el marco de sus competencias como autoridad responsable de la supervisión de la entidad de crédito participada y, en particular, valorando la influencia de la fundación bancaria sobre la gestión sana y prudente de la citada entidad, de conformidad con los criterios establecidos en el régimen de participaciones significativas previsto en el citado título VI de la Ley 26/1988, de 29 de julio, sobre Disciplina e Intervención de las Entidades de Crédito.

2. A los efectos de las funciones de supervisión asignadas en el apartado anterior, el Banco de España podrá:

a) Realizar las inspecciones y las comprobaciones que considere oportunas en el ejercicio de sus funciones.

b) Requerir a la fundación bancaria cuanta información resulte necesaria para desarrollar sus funciones.

El acceso a las informaciones y datos requeridos por el Banco de España se encuentra amparado por el artículo 11.2.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

3. Asimismo, el Ministro de Economía y Competitividad, o el Banco de España con su habilitación expresa, podrá desarrollar las normas y modelos a que deberá sujetarse la contabilidad de las fundaciones bancarias.

Para el establecimiento y modificación de las señaladas normas y modelos será preceptivo el informe previo del Instituto de Contabilidad y Auditoría de Cuentas.

[. . .]

§ 45

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 295, de 10 de diciembre de 2013
Última modificación: 9 de julio de 2022
Referencia: BOE-A-2013-12887

[. . .]

TÍTULO I

Transparencia de la actividad pública

[. . .]

CAPÍTULO II

Publicidad activa

Artículo 5. *Principios generales.*

1. Los sujetos enumerados en el artículo 2.1 publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública.

2. Las obligaciones de transparencia contenidas en este capítulo se entienden sin perjuicio de la aplicación de la normativa autonómica correspondiente o de otras disposiciones específicas que prevean un régimen más amplio en materia de publicidad.

3. Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos.

4. La información sujeta a las obligaciones de transparencia será publicada en las correspondientes sedes electrónicas o páginas web y de una manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada así como su identificación y localización.

Cuando se trate de entidades sin ánimo de lucro que persigan exclusivamente fines de interés social o cultural y cuyo presupuesto sea inferior a 50.000 euros, el cumplimiento de las obligaciones derivadas de esta Ley podrá realizarse utilizando los medios electrónicos puestos a su disposición por la Administración Pública de la que provenga la mayor parte de las ayudas o subvenciones públicas percibidas.

5. Toda la información será comprensible, de acceso fácil y gratuito y estará a disposición de las personas con discapacidad en una modalidad suministrada por medios o en formatos adecuados de manera que resulten accesibles y comprensibles, conforme al principio de accesibilidad universal y diseño para todos.

[. . .]

CAPÍTULO III

Derecho de acceso a la información pública

[. . .]

Artículo 15. *Protección de datos personales.*

1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.

2. Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano.

3. Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal.

Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios:

a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.

d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

4. No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas.

5. La normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso.

[. . .]

TÍTULO III

Consejo de Transparencia y Buen Gobierno

Artículo 33. *Consejo de Transparencia y Buen Gobierno.*

1. Se crea el Consejo de Transparencia y Buen Gobierno como organismo público de los previstos en la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Estará adscrito al Ministerio de Hacienda y Administraciones Públicas.

2. El Consejo de Transparencia y Buen Gobierno tiene personalidad jurídica propia y plena capacidad de obrar. Actúa con autonomía y plena independencia en el cumplimiento de sus fines.

[. . .]

Artículo 36. *Comisión de Transparencia y Buen Gobierno.*

1. La Comisión de Transparencia y Buen Gobierno ejercerá todas las competencias que le asigna esta Ley, así como aquellas que les sean atribuidas en su normativa de desarrollo.

2. Dicha Comisión estará compuesta por:

a) El Presidente.
b) Un Diputado.
c) Un Senador.
d) Un representante del Tribunal de Cuentas.
e) Un representante del Defensor del Pueblo.
f) Un representante de la Agencia Española de Protección de Datos.
g) Un representante de la Secretaría de Estado de Administraciones Públicas.
h) Un representante de la Autoridad Independiente de Responsabilidad Fiscal.

3. La condición de miembro de la Comisión del Consejo de Transparencia y Buen Gobierno no exigirá dedicación exclusiva ni dará derecho a remuneración con excepción de lo previsto en el artículo siguiente.

4. Al menos una vez al año, la Comisión de Transparencia y Buen Gobierno convocará a los representantes de los organismos que, con funciones similares a las desarrolladas por ella, hayan sido creados por las Comunidades Autónomas en ejercicio de sus competencias. A esta reunión podrá ser convocado un representante de la Administración Local propuesto por la Federación Española de Municipios y Provincias.

[. . .]

Disposición adicional quinta. *Colaboración con la Agencia Española de Protección de Datos.*

El Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adoptarán conjuntamente los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de esta Ley, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en esta Ley y en la Ley Orgánica 15/1999, de 13 de diciembre.

[. . .]

§ 46

Ley 4/2013, de 4 de junio, de medidas de flexibilización y fomento del mercado del alquiler de viviendas. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 134, de 5 de junio de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-5941

[. . .]

Artículo tercero. *Registro de sentencias firmes de impagos de rentas de alquiler.*

1. Se crea un Registro de sentencias firmes de impagos de rentas de alquiler. Por real decreto se regulará su organización y funcionamiento.

2. Con la finalidad de ofrecer información sobre el riesgo que supone arrendar inmuebles a personas que tienen precedentes de incumplimiento de sus obligaciones de pago de renta en contratos de arrendamiento y que, por dicho motivo, hayan sido condenadas por sentencia firme en un procedimiento de desahucio del artículo 250.1.1.° o del artículo 438 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, el secretario judicial correspondiente remitirá dicha información al Registro de sentencias firmes de impagos de rentas de alquiler.

3. En el mismo sentido, los órganos de arbitraje competentes deberán poner en conocimiento de dicho Registro los datos relativos a aquellas personas que hayan sido declaradas responsables del impago de rentas de arrendamientos, por medio de laudo arbitral dictado al efecto.

4. Tendrán acceso a la información obrante en el Registro, los propietarios de inmuebles que deseen suscribir contratos de arrendamiento sobre los mismos, sean personas físicas o jurídicas. A tales efectos deberán presentar una propuesta de contrato de arrendamiento en la que se identifique al eventual arrendatario, limitándose la información a la que tendrá derecho, a los datos que consten en el Registro, relacionados exclusivamente con dicho arrendatario.

5. Las personas incluidas en el Registro podrán instar la cancelación de la inscripción cuando en el proceso correspondiente hubieran satisfecho la deuda por la que fueron condenadas. No obstante, la constancia en el citado Registro tendrá una duración máxima de seis años, procediéndose a su cancelación automática a la finalización de dicho plazo.

6. La inscripción a la que se refiere este artículo estará, en todo caso sujeta a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Disposición adicional primera. *Transmisión de información sobre contratos de arrendamiento de vivienda.*

Con la finalidad de definir, proponer y ejecutar la política del Gobierno relativa al acceso a la vivienda, el Ministerio de Fomento podrá articular instrumentos de colaboración que le permitan obtener información acerca de la localización de las viviendas, de los contratos de arrendamiento sobre las mismas de los que se tenga constancia a través de los Registradores de la Propiedad, de los registros administrativos de contratos de arrendamiento o de depósitos de fianzas de las Comunidades Autónomas y del Consejo General del Notariado, así como de aquellos datos de carácter estadístico que consten en la Administración Tributaria derivados del acceso a beneficios fiscales de arrendadores y arrendatarios. En ningún caso, dicha información contendrá datos de carácter personal protegidos por la legislación en materia de protección de datos.

[. . .]

§ 47

Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 134, de 5 de junio de 2013
Última modificación: 23 de enero de 2025
Referencia: BOE-A-2013-5940

[. . .]

CAPÍTULO II

Funciones

[. . .]

Artículo 8. *Supervisión y control del mercado postal.*

La Comisión Nacional de los Mercados y la Competencia supervisará y controlará el correcto funcionamiento del mercado postal. En particular, ejercerá las siguientes funciones:

1. Velar para que se garantice el servicio postal universal, en cumplimiento de la normativa postal y la libre competencia en el sector, ejerciendo las funciones y competencias que le atribuye la legislación vigente, sin perjuicio de lo indicado en la Disposición adicional undécima de esta Ley.

2. Verificar la contabilidad analítica del operador designado y el coste neto del servicio postal universal y determinar la cuantía de la carga financiera injusta de la prestación de dicho servicio de conformidad con lo establecido en el Capítulo III del Título III de la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal, así como en su normativa de desarrollo.

3. Gestionar el Fondo de financiación del servicio postal universal y las prestaciones de carácter público afectas a su financiación de conformidad con lo establecido en el Capítulo III del Título III de la Ley 43/2010, de 30 de diciembre, y en su normativa de desarrollo.

4. Supervisar y controlar la aplicación de la normativa vigente en materia de acceso a la red y a otras infraestructuras y servicios postales, de conformidad con lo establecido en el Título V de la Ley 43/2010, de 30 de diciembre, así como en su normativa de desarrollo.

5. Realizar el control y medición de las condiciones de prestación del servicio postal universal, de conformidad con lo establecido en el Capítulo II del Título III de la Ley 43/2010, de 30 de diciembre, así como en su normativa de desarrollo.

6. Gestionar y controlar la utilización del censo promocional conforme a lo definido en el artículo 31 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, conforme a lo que se determine reglamentariamente.

7. Dictar circulares para las entidades que operen en el sector postal, que serán vinculantes una vez publicadas en el «Boletín Oficial del Estado».

8. Emitir el informe previsto en la Disposición adicional segunda de la Ley 43/2010, de 30 de diciembre, para el seguimiento de las condiciones de prestación del servicio postal universal.

9. Realizar cualesquiera otras funciones que le sean atribuidas por Ley o por Real Decreto.

[. . .]

§ 48

Ley 33/2011, de 4 de octubre, General de Salud Pública. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 240, de 5 de octubre de 2011
Última modificación: 23 de marzo de 2023
Referencia: BOE-A-2011-15623

[. . .]

TÍTULO I

Derechos, deberes y obligaciones en salud pública

CAPÍTULO I

Derechos de los ciudadanos

[. . .]

Artículo 7. *Derecho a la intimidad, confidencialidad y respeto de la dignidad.*

1. Todas las personas tienen derecho al respeto de su dignidad e intimidad personal y familiar en relación con su participación en actuaciones de salud pública.

2. La información personal que se emplee en las actuaciones de salud pública se regirá por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en la Ley 41/2002, de 14 de noviembre, básica reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica.

[. . .]

CAPÍTULO IX

Sistema de Información en Salud Pública

[. . .]

Artículo 42. *Datos básicos y comunicación de la información.*

1. El Consejo Interterritorial del Sistema Nacional de Salud aprobará la información sobre salud pública que se incluya en el Sistema de Información en salud pública, a cuyo efecto definirá un conjunto de datos básicos en las condiciones y requisitos establecidos en el capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

2. El acceso a la información por parte de los usuarios del sistema se realizará en los términos establecidos en esta ley y sus disposiciones de desarrollo.

[. . .]

§ 49

Ley 29/2011, de 22 de septiembre, de Reconocimiento y Protección Integral a las Víctimas del Terrorismo. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 229, de 23 de septiembre de 2011
Última modificación: 29 de diciembre de 2021
Referencia: BOE-A-2011-15039

[. . .]

TÍTULO CUARTO

Régimen de protección social

[. . .]

Artículo 42. *De la protección de datos y las limitaciones a la publicidad.*

En las actuaciones y procedimientos relacionados con el terrorismo, se protegerá la intimidad de las víctimas; en especial sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia.

[. . .]

§ 50

Ley 26/2011, de 1 de agosto, de adaptación normativa a la Convención Internacional sobre los Derechos de las Personas con Discapacidad. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 184, de 2 de agosto de 2011
Última modificación: 31 de octubre de 2015
Referencia: BOE-A-2011-13241

[. . .]

Disposición adicional segunda. *Suministro de información de las Comunidades Autónomas.*

De acuerdo con los principios de información mutua y colaboración entre Administraciones públicas y con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y con el fin de garantizar el cumplimiento de las obligaciones previstas en tratados y convenios internacionales, las Comunidades Autónomas, en el ámbito de sus competencias, remitirán anualmente al Ministerio de Sanidad, Política Social e Igualdad, datos estadísticos sobre la situación de las personas con discapacidad, en la forma que se establezca reglamentariamente. La aportación de los datos relativos al empleo y a las condiciones de trabajo de las personas con discapacidad se regirá por su normativa específica.

[. . .]

§ 51

Ley 23/2011, de 29 de julio, de depósito legal. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: 5 de mayo de 2022
Referencia: BOE-A-2011-13114

CAPÍTULO I

Disposiciones generales

[. . .]

Artículo 2. *Objetivos del depósito legal.*

Son objetivos del depósito legal:

1. Recopilar, almacenar y conservar, en los centros de conservación de la Administración General del Estado y de las Comunidades Autónomas, las publicaciones que constituyen el patrimonio bibliográfico, sonoro, visual, audiovisual y digital español, con objeto de preservarlo y legarlo a las generaciones futuras, velar por su difusión y permitir el acceso al mismo para garantizar el derecho de acceso a la cultura, a la información y a la investigación.

2. Recoger la información precisa para confeccionar las estadísticas oficiales sobre el patrimonio de referencia.

3. Describir el conjunto de la producción bibliográfica, sonora, visual, audiovisual y digital española, con el fin de difundirla, y posibilitar el intercambio de datos con otras agencias o instituciones bibliotecarias españolas y extranjeras.

4. Permitir el acceso y la consulta de las publicaciones almacenadas, bien en las instalaciones de los propios centros de conservación o bien a través de bases de datos en línea de acceso restringido, asegurando su correcta conservación y respetando en todo caso la legislación sobre propiedad intelectual; protección de datos; de la lectura, del libro y de las bibliotecas; accesibilidad; así como lo dispuesto en esta ley.

[. . .]

CAPÍTULO II

De la obligación del depósito legal

[. . .]

Artículo 5. *Publicaciones excluidas del depósito legal.*

No serán objeto de depósito legal las siguientes publicaciones en soporte tangible:

a) Documentos de las Administraciones Públicas de carácter interno o que resulten susceptibles de integración en expedientes administrativos.

b) Documentos de instituciones y organizaciones, incluidas las empresariales, que versen únicamente sobre asuntos internos y estén dirigidas al personal de las mismas, tales como circulares, instrucciones o manuales de procedimiento.

c) Publicaciones destinadas a concursos de promoción o traslado de los cuerpos o escalas de las distintas administraciones públicas.

d) Sellos de correo.

e) Impresos de carácter social como invitaciones de boda y bautizo, esquelas de defunción, tarjetas de visita, carnés de identidad, títulos o diplomas.

f) Impresos de oficinas, formularios, incluidos los oficiales, cuestionarios y encuestas no cumplimentadas, excepto que complementen una obra cuyo contenido sea técnico o científico, por ejemplo, un volumen formado por una recopilación de formularios que acompaña a un libro sobre procedimiento administrativo.

g) Dosieres de prensa.

h) Publicaciones comerciales publicitarias.

i) Catálogos comerciales de todo tipo, con la excepción de los catálogos de editoriales, librerías y subastas.

j) Calendarios y agendas.

k) Objetos tridimensionales, aunque acompañen a un documento principal.

l) Manuales de instrucciones de objetos, electrodomésticos, maquinaria o análogos.

m) Todo producto de un sistema informático que contenga datos que afecten a la privacidad de personas físicas y jurídicas y cuantos estén incluidos en la normativa de protección de datos personales.

n) Programas audiovisuales emitidos por prestadores del servicio de comunicación audiovisual, salvo que sean objeto de distribución.

ñ) Pasatiempos, crucigramas, sudokus, sopas de letras y similares.

o) Estampas originales realizadas con cualquier técnica.

p) Fotografías editadas.

q) Publicaciones de impresión bajo demanda destinadas a distribución en un ámbito familiar.

[. . .]

Artículo 8. *Sujetos obligados a constituir el depósito legal en el caso de publicaciones electrónicas y publicaciones en línea.*

1. La responsabilidad del depósito legal de las publicaciones electrónicas a las que se refiere el artículo 4 recaerá en su editor o productor.

2. Sin perjuicio del apartado anterior, se exonera a los editores de publicaciones en línea de la gestión del depósito legal. En todo caso, estarán obligados a facilitar la recolección automática de dichas publicaciones cuando estén libremente accesibles en Internet o transferir las publicaciones de acceso restringido que les sean solicitadas por los centros de conservación, que serán quienes determinen qué publicaciones en línea y qué recursos se capturarán o depositarán.

En el caso de que los editores hubieran adoptado soluciones tecnológicas, para evitar accesos o utilizaciones no autorizadas de sus publicaciones, la entrega o transferencia de estas publicaciones se realizará de acuerdo a las condiciones adecuadas que permitan su conservación y acceso por parte de los centros de conservación, quienes garantizarán en todo caso la protección de los derechos de autor de acuerdo a los términos establecidos en la legislación vigente en materia de propiedad intelectual, así como la protección de datos de carácter personal.

[. . .]

§ 52

Ley Orgánica 9/2011, de 27 de julio, de derechos y deberes de los miembros de las Fuerzas Armadas. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 180, de 28 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-12961

[. . .]

TÍTULO I

Del ejercicio de los derechos fundamentales y libertades públicas

[. . .]

Artículo 10. *Derecho a la intimidad y dignidad personal.*

1. El militar tiene derecho a la intimidad personal. En el ejercicio y salvaguarda de este derecho se tendrán en cuenta las circunstancias en que tengan lugar las operaciones.

También tiene derecho al secreto de las comunicaciones y a la inviolabilidad del domicilio, incluido el ubicado dentro de unidades, en los términos establecidos en la Constitución y en el resto del ordenamiento jurídico.

Se deberá respetar la dignidad personal y en el trabajo de todo militar, especialmente frente al acoso, tanto sexual y por razón de sexo como profesional.

2. Las revistas e inspecciones deberán respetar en todo caso los derechos contenidos en el apartado anterior.

Como norma general, el registro personal de los militares, de sus taquillas, efectos y pertenencias que estuvieren en la unidad requerirá del consentimiento del afectado o resolución judicial. No obstante, cuando existan indicios de la comisión de un hecho delictivo o por razones fundadas de salud pública o de seguridad, el jefe de la unidad podrá autorizar tales registros de forma proporcionada y expresamente motivada. Estos registros se realizarán con la asistencia del interesado y en presencia de al menos dos testigos o sólo de éstos, si el interesado debidamente notificado no asistiera.

3. Los datos relativos a los miembros de las Fuerzas Armadas estarán sujetos a la legislación sobre protección de datos de carácter personal. A tal efecto los poderes públicos llevarán a cabo las acciones necesarias para la plena efectividad de este derecho fundamental, especialmente cuando concurran circunstancias que pudieran incidir en la seguridad de los militares.

[. . .]

§ 53

Ley 20/2011, de 21 de julio, del Registro Civil. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 175, de 22 de julio de 2011
Última modificación: 3 de enero de 2025
Referencia: BOE-A-2011-12628

TÍTULO I

El Registro Civil. Disposiciones generales

CAPÍTULO PRIMERO

Naturaleza, contenido y competencias del Registro Civil

[. . .]

Artículo 3. *Elementos definitorios del Registro Civil.*

1. El Registro Civil es único para toda España.

2. El Registro Civil es electrónico. Los datos serán objeto de tratamiento automatizado y se integrarán en una base de datos única cuya estructura, organización y funcionamiento es competencia del Ministerio de Justicia conforme a la presente Ley y a sus normas de desarrollo.

3. Serán de aplicación al Registro Civil las medidas de seguridad establecidas en la normativa vigente en materia de protección de datos de carácter personal.

[. . .]

Disposición adicional novena. *Obtención de datos del Instituto Nacional de Estadística.*

Para facilitar la tramitación telemática a los Registros Civiles, el Instituto Nacional de Estadística dará acceso telemático a los datos de domicilio relativos al Padrón municipal que guarden relación con los hechos inscribibles, así como, si fuera necesario para la correcta identificación de los citados hechos, a los datos de identificación que figuren en las inscripciones padronales, sin precisar para todo ello del consentimiento del interesado.

También se utilizarán los datos padronales para la actualización de la información obrante en las bases de datos de los Registros Civiles, en idénticas condiciones que en el párrafo anterior.

[. . .]

Disposición final quinta bis. *Aranceles notariales.*

El Gobierno aprobará los aranceles correspondientes a la intervención de los Notarios en la tramitación de las actas matrimoniales previas y por la celebración de matrimonios en forma civil con la autorización de las escrituras públicas correspondientes.

[. . .]

§ 54

Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 131, de 2 de junio de 2011
Última modificación: 11 de enero de 2023
Referencia: BOE-A-2011-9617

[. . .]

TÍTULO II

Recursos humanos dedicados a la investigación

CAPÍTULO I

Personal Investigador al servicio de las Universidades públicas, de los Organismos Públicos de Investigación y de los Organismos de investigación de otras Administraciones Públicas

[. . .]

Artículo 15. *Deberes del personal investigador.*

1. Los deberes del personal investigador que preste servicios en universidades públicas, en Organismos Públicos de Investigación de la Administración General del Estado o en organismos de investigación de otras Administraciones Públicas serán los siguientes:

a) Observar las prácticas éticas reconocidas, los principios éticos correspondientes a sus disciplinas, y la integridad de la investigación, así como las normas éticas recogidas en los diversos códigos deontológicos aplicables.

b) Evitar el plagio y la apropiación indebida de la autoría de trabajos científicos o tecnológicos de terceros.

c) Poner en conocimiento de las entidades para las que presta servicios todos los hallazgos, descubrimientos y resultados susceptibles de protección jurídica, y colaborar en los procesos de protección y de transferencia de los resultados de sus investigaciones.

d) Difundir los resultados de sus investigaciones, en su caso, según lo indicado en esta ley, para que los resultados se aprovechen mediante la comunicación y la transferencia a otros contextos de investigación, sociales o tecnológicos, y si procede, para su comercialización y valorización. En especial, el personal investigador deberá velar y tomar la iniciativa para que sus resultados generen valor social.

e) Procurar que su labor sea relevante para la sociedad.

f) Participar en las reuniones y actividades de los órganos de gobierno y de gestión de los que forme parte, y en los procesos de evaluación y mejora para los que se le requiera.

g) Encaminar sus investigaciones hacia el logro de los objetivos estratégicos de las entidades para las que presta servicios, y obtener o colaborar en los procesos de obtención de los permisos y autorizaciones necesarias antes de iniciar su labor.

h) Informar a las entidades para las que presta servicios o que financian o supervisan su actividad de posibles retrasos y redefiniciones en los proyectos de investigación de los que sea responsable, así como de la finalización de los proyectos, o de la necesidad de abandonar o suspender los proyectos antes de lo previsto.

i) Rendir cuentas sobre su trabajo a las entidades para las que presta servicios o que financian o supervisan su actividad, y responsabilizarse del uso eficaz de la financiación de los proyectos de investigación que desarrolle. Para ello, deberá observar los principios de gestión correcta, transparente y eficaz, y cooperar en las auditorías sobre sus investigaciones que procedan según la normativa vigente.

j) Utilizar la denominación de las entidades para las que presta servicios en la realización de su actividad científica, de acuerdo con la normativa interna de dichas entidades y los acuerdos, pactos y convenios que estas suscriban.

k) Seguir en todo momento prácticas de trabajo seguras de acuerdo con la normativa aplicable, incluida la adopción de las precauciones necesarias en materia de prevención de riesgos laborales, y velar por que el personal a su cargo cumpla con estas prácticas.

l) Adoptar las medidas necesarias para el cumplimiento de la normativa aplicable en materia de protección de datos y de confidencialidad.

m) Seguir en todo momento prácticas igualitarias de acuerdo con la normativa aplicable, incluida la adopción de las precauciones necesarias en materia de prevención de cualquier tipo de discriminación, y velar por que el personal a su cargo cumpla con estas prácticas.

2. Lo dispuesto en este artículo se entenderá sin perjuicio de lo establecido por el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, así como de las restantes normas que resulten de aplicación al personal investigador, en función del tipo de entidad para la que preste servicios y de la actividad realizada.

[. . .]

CAPÍTULO II

Especificidades aplicables al personal al servicio de los Organismos Públicos de Investigación de la Administración General del Estado

[. . .]

Sección 2.ª Personal de investigación al servicio de los organismos públicos de Investigación de la Administración General del Estado

[. . .]

Artículo 28. *Derechos y deberes del personal técnico al servicio de los Organismos Públicos de Investigación de la Administración General del Estado.*

1. Serán de aplicación al personal técnico al servicio de los Organismos Públicos de Investigación de la Administración General del Estado los artículos 16.1 y 2 de esta ley. Además, serán de aplicación al personal técnico funcionario de carrera o laboral fijo al servicio de los Organismos Públicos de Investigación de la Administración General del Estado los artículos 17, 18 y 19 de esta ley.

2. El personal técnico que preste servicios en Organismos Públicos de Investigación de la Administración General del Estado tendrá los siguientes derechos:

a) A determinar libremente los métodos de resolución de problemas, dentro del marco de las prácticas y los principios éticos reconocidos y de la normativa aplicable sobre propiedad intelectual, y teniendo en cuenta las posibles limitaciones derivadas de las circunstancias de la actividad y del entorno, de las actividades de supervisión, orientación o gestión, de las limitaciones presupuestarias o de las infraestructuras.

b) A ser reconocido y amparado en la autoría o coautoría de los trabajos de carácter técnico en los que participe.

c) Al respeto al principio de igualdad de género en el desempeño de sus funciones, en la contratación de personal y en el desarrollo de su carrera profesional.

d) A contar con los medios e instalaciones adecuados para el desarrollo de sus funciones, dentro de los límites derivados de la aplicación de los principios de eficacia y eficiencia en la asignación, utilización y gestión de dichos medios e instalaciones por la entidad para la que preste servicios, y dentro de las disponibilidades presupuestarias.

e) A la consideración y respeto de su actividad.

f) A utilizar la denominación de las entidades para las que presta servicios en la realización de su actividad.

g) A participar en los beneficios que obtengan las entidades para las que presta servicios, como consecuencia de la eventual explotación de los resultados de la actividad en que haya participado el personal técnico. Los referidos beneficios no tendrán en ningún caso naturaleza retributiva o salarial para el personal técnico.

h) A participar en los programas favorecedores de la conciliación entre la vida personal, familiar y laboral que pongan en práctica las entidades para las que presta servicios.

i) A su desarrollo profesional, mediante el acceso a medidas de formación continua para el desarrollo de sus capacidades y competencias.

Estos derechos se entenderán sin perjuicio de los establecidos por la Ley 7/2007, de 12 de abril, así como de los restantes derechos que resulten de aplicación al personal técnico, en función del tipo de entidad para la que preste servicios y de la actividad realizada.

3. Los deberes del personal técnico que preste servicios en Organismos Públicos de Investigación de la Administración General del Estado serán los siguientes:

a) Observar las prácticas éticas reconocidas y los principios éticos correspondientes a sus disciplinas, así como las normas éticas recogidas en los diversos códigos deontológicos aplicables.

b) Poner en conocimiento de las entidades para las que presta servicios todos los hallazgos, descubrimientos y resultados susceptibles de protección jurídica, y colaborar en los procesos de protección y de transferencia de los resultados de su actividad.

c) Participar en las reuniones y actividades de los órganos de gobierno y de gestión de los que forme parte y en los procesos de evaluación y mejora para los que se le requiera.

d) Procurar que su labor sea relevante para la sociedad.

e) Utilizar la denominación de las entidades para las que presta servicios en la realización de su actividad, de acuerdo con la normativa interna de dichas entidades y los acuerdos, pactos y convenios que éstas suscriban.

f) Seguir en todo momento prácticas de trabajo seguras de acuerdo con la normativa aplicable, incluida la adopción de las precauciones necesarias en materia de prevención de riesgos laborales, y velar por que el personal a su cargo cumpla con estas prácticas.

g) Adoptar las medidas necesarias para el cumplimiento de la normativa aplicable en materia de protección de datos y de confidencialidad.

Estos deberes se entenderán sin perjuicio de los establecidos por la Ley 7/2007, de 12 de abril, así como de los restantes deberes que resulten de aplicación al personal técnico, en función del tipo de entidad para la que preste servicios y de la actividad realizada.

[. . .]

Información relacionada

- Las referencias contenidas en la presente Ley, a la Estrategia Española de Ciencia y Tecnología, a la Estrategia Española de Innovación, al Plan Estatal de Investigación Científica y Técnica y al Plan Estatal de Innovación, se entenderán efectuadas, respectivamente, a la Estrategia Española de Ciencia, Tecnología e Innovación y al Plan Estatal de Investigación Científica y Técnica y de Innovación, según establece la disposición adicional 1 de la Ley 17/2022, de 5 de septiembre. Ref. BOE-A-2022-14581
- Las referencias contenidas en la presente Ley al Centro para el Desarrollo Tecnológico e Industrial E.P.E., se entenderán realizadas en todo caso al Centro para el Desarrollo Tecnológico y la Innovación, según establece la disposición adicional 2 de la Ley 17/2022, de 5 de septiembre. Ref. BOE-A-2022-14581

§ 55

Ley 13/2011, de 27 de mayo, de regulación del juego. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 127, de 28 de mayo de 2011
Última modificación: 31 de diciembre de 2022
Referencia: BOE-A-2011-9280

[. . .]

TÍTULO IV

Control de la actividad

[. . .]

CAPÍTULO II

Participantes

Artículo 15. *Derechos y obligaciones de los participantes en los juegos.*

1. Los participantes en los juegos tienen los siguientes derechos:

a) A obtener información clara y veraz sobre las reglas del juego en el que deseen participar.

b) A cobrar los premios que les pudieran corresponder en el tiempo y forma establecidos, de conformidad con la normativa específica de cada juego.

c) A formular ante la Comisión Nacional del Juego las reclamaciones contra las decisiones del operador que afecten a sus intereses.

d) Al tiempo de uso correspondiente al precio de la partida de que se trate.

e) A jugar libremente, sin coacciones o amenazas provenientes de otros jugadores o de cualquier otra tercera persona.

f) A conocer en cualquier momento el importe que ha jugado o apostado, así como en el caso de disponer de una cuenta de usuario abierta en el operador de juego, a conocer el saldo de la misma.

g) A identificarse de modo seguro mediante el documento nacional de identidad, pasaporte o documento equivalente o mediante sistema de firma electrónica reconocida, así como a la protección de sus datos personales conforme a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

h) A conocer en todo momento la identidad del operador de juego, especialmente en el caso de juegos telemáticos, así como a conocer, en el caso de reclamaciones o posibles infracciones, la identidad del personal que interactúe con los participantes.

i) A recibir información sobre la práctica responsable del juego.

2. Los participantes en los juegos tienen las siguientes obligaciones:

a) Identificarse ante los operadores de juego en los términos que reglamentariamente se establezcan.

b) Cumplir las normas y reglas que, en relación con los participantes, se establezcan en las órdenes ministeriales que se aprueben de conformidad con el artículo 5 de esta Ley.

c) No alterar el normal desarrollo de los juegos.

3. La relación entre el participante y el operador habilitado constituye una relación de carácter privado, y por tanto, las disputas o controversias que pudieran surgir entre ellos estarán sujetas a los Juzgados y Tribunales del orden jurisdiccional civil, sin perjuicio del ejercicio de la potestad sancionadora ejercida por la Comisión Nacional del Juego dentro de las competencias reconocidas en esta Ley.

4. Los operadores habilitados establecerán los procedimientos adecuados para mantener la privacidad de los datos de los usuarios de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa complementaria.

Los operadores únicamente tratarán los datos de los participantes que fueran necesarios para el adecuado desarrollo de la actividad de juego para la que hubieran sido autorizados y para el cumplimiento de las obligaciones establecidas en esta Ley. Los datos serán cancelados una vez cumplidas las finalidades que justificaron su tratamiento.

En todo caso, de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, los operadores deberán informar a los usuarios acerca del tratamiento de sus datos de carácter personal y las finalidades para las que se produce el tratamiento, así como los derechos que les corresponden de conformidad con la normativa vigente en materia de protección de datos de carácter personal.

Los operadores deberán asimismo implantar sobre los ficheros y tratamientos las medidas de seguridad establecidas en la normativa vigente en materia de protección de datos y dar cumplimiento al deber de secreto impuesto por dicha normativa.

CAPÍTULO III

Homologación de los sistemas técnicos de juego

Artículo 16. *Homologación de los sistemas técnicos de juego.*

1. Las entidades que lleven a cabo la organización, explotación y desarrollo de juegos regulados en esta Ley dispondrán del material software, equipos, sistemas, terminales e instrumentos en general necesarios para el desarrollo de estas actividades, debidamente homologados.

2. La homologación de los sistemas técnicos de juego, así como el establecimiento de las especificaciones necesarias para su funcionamiento, corresponde a la Comisión Nacional del Juego, que aprobará en el marco de los criterios fijados por el Ministerio de Economía y Hacienda y el Consejo de Políticas del Juego, el procedimiento de certificación de los sistemas técnicos de juego incluyendo, en su caso, las homologaciones de material de juego. La Comisión Nacional del Juego velará para que el establecimiento de las especificaciones, así como los procedimientos de certificación y homologación de material de juego, no introduzcan obstáculos que pudieren distorsionar injustificadamente la competencia en el mercado.

3. Las homologaciones y certificaciones validadas por los órganos competentes de las Comunidades Autónomas para la concesión de títulos habilitantes de ámbito autonómico, podrán tener efectos en los procedimientos regulados en esta Ley en los términos que reglamentariamente se establezcan.

4. En los procedimientos de homologación de los sistemas técnicos de juego que puedan afectar de manera relevante al tratamiento de datos de carácter personal por parte de los

operadores, la Comisión Nacional del Juego solicitará informe a la Agencia Española de Protección de Datos.

[. . .]

TÍTULO V

La Administración del Juego

[. . .]

Artículo 22. *Los Registros del sector del juego.*

1. La Comisión Nacional del Juego constituirá, bajo su dependencia y control, los siguientes Registros de ámbito estatal:

a) El Registro General de Licencias de Juego, en el que se practicarán las inscripciones de carácter provisional de las empresas que participen en los procedimientos concurrenciales de licencias generales, así como las inscripciones de carácter definitivo de las entidades que hayan obtenido una licencia para desarrollar la actividad de juego.

b) El Registro General de Interdicciones de Acceso al Juego, en el que se inscribirá la información necesaria para hacer efectivo el derecho de los ciudadanos a que les sea prohibida la participación en las actividades de juego en los casos en que sea necesaria la identificación para la participación en las mismas. Asimismo, se inscribirá la información relativa a aquellas otras personas que, por resolución judicial tengan prohibido el acceso al juego o se hallen incapacitadas legalmente. Los requisitos de carácter subjetivo preceptivos para la inscripción en este registro serán determinados por la Comisión Nacional del Juego. La información de este registro se facilitará a los operadores de juego con la finalidad de impedir el acceso al juego de las personas inscritas en el mismo.

Reglamentariamente se establecerá el procedimiento para coordinar la comunicación de datos entre los Registros de Interdicción de Acceso al Juego de las distintas Comunidades Autónomas y el Registro General de Interdicciones de Acceso al Juego.

c) Registro de Personas Vinculadas a Operadores de Juego, en el que se inscribirán los datos de los accionistas, partícipes o titulares significativos de la propia empresa de juego, su personal directivo y empleados directamente involucrados en el desarrollo de los juegos, así como sus cónyuges o personas con las que convivan, ascendientes y descendientes en primer grado.

2. El tratamiento de los datos de carácter personal en los ficheros y registros a los que se refiere el apartado anterior, para los fines previstos en esta Ley, no requerirá del consentimiento de sus titulares.

Reglamentariamente se determinará el contenido concreto de los registros a los que se refiere el presente artículo. Los registros no incluirán más datos que los estrictamente necesarios para el cumplimiento de las finalidades previstas para los mismos en esta Ley.

El contenido de los registros referidos en el presente artículo no presenta carácter público, quedando limitada la comunicación de los datos contenidos en los mismos, única y exclusivamente, a las finalidades previstas en esta Ley.

3. Reglamentariamente se establecerá la organización y funcionamiento de los registros del sector del juego. En este marco, la Comisión Nacional del Juego y los órganos competentes de las Comunidades Autónomas podrán acordar, mediante los oportunos convenios de colaboración, la interconexión de sus registros de juego y el intercambio de datos e información tributaria, con pleno respeto a la normativa reguladora de la protección de datos de carácter personal.

[. . .]

Artículo 24. *Inspección y Control.*

1. Al objeto de garantizar lo dispuesto en esta Ley y en las disposiciones que la complementen, corresponderá a la Comisión Nacional del Juego la auditoría, vigilancia, inspección y control de todos los aspectos y estándares administrativos, económicos,

procedimentales, técnicos, informáticos, telemáticos y de documentación, relativos al desarrollo de las actividades previstas en esta Ley.

Asimismo, corresponderá a la Comisión Nacional del Juego la investigación y persecución de los juegos ilegales, sin perjuicio de las facultades que correspondan a las Fuerzas y Cuerpos de Seguridad competentes y al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias en los términos del artículo 45.4 f) de la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo. La Comisión Nacional del Juego establecerá los procedimientos necesarios en orden al cumplimiento de las funciones antes citadas.

Las Fuerzas y Cuerpos de Seguridad del Estado, de acuerdo con lo establecido en el artículo 12.1.A), letra d), de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, colaborarán con la Comisión Nacional del Juego en las funciones de vigilancia e inspección del cumplimiento de la normativa en materia de juego. Si como resultado de la actividad inspectora llevada a cabo por las Fuerzas y Cuerpos de Seguridad del Estado en el ejercicio de las funciones de colaboración con la Comisión Nacional del Juego se comprobara la existencia de indicios de la comisión de una infracción, se levantará la oportuna acta que será enviada a los órganos competentes para iniciar el procedimiento sancionador.

2. Por la Comisión Nacional del Juego se establecerán los procedimientos adicionales para el seguimiento y control de los operadores que realicen actividades de juego sujetas a reserva en virtud de una ley y del cumplimiento de las condiciones que se establezcan a los mismos, en especial, en relación con la protección del orden público y la prevención del blanqueo de capitales y financiación del terrorismo. En el supuesto de que, en el ejercicio de su labor inspectora, la Comisión Nacional del Juego apreciara posibles infracciones de las obligaciones establecidas en la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo, informará a la Secretaría de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias en los términos del artículo 48.1 de la citada Ley.

3. La Comisión Nacional del Juego podrá efectuar un control sobre la cuenta de usuario del participante en las actividades de juego objeto de esta Ley, así como de los operadores o proveedores de servicios de juego. La Comisión Nacional del Juego tendrá acceso a los datos de carácter personal recogidos en la cuenta de usuario de los participantes, respetando en todo momento lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos y su normativa de desarrollo.

Las Administraciones Públicas darán acceso a la Comisión Nacional del Juego a sus bases de datos con la finalidad de comprobar la identidad del participante y, especialmente, su condición de mayor de edad.

4. Los operadores habilitados, sus representantes legales y el personal que en su caso se encuentre al frente de las actividades en el momento de la inspección, tendrán la obligación de facilitar a los inspectores y a su personal auxiliar el acceso a los locales y a sus diversas dependencias, así como el examen de los soportes técnicos e informáticos, libros, registros y documentos que solicite la inspección. El resultado de la inspección se hará constar en acta que tendrá la naturaleza de documento público y hará prueba, salvo que se acredite lo contrario, de los hechos y circunstancias que la motiven.

El acta deberá ser firmada por el funcionario que la extienda y por la persona o representante de la entidad fiscalizada, quien podrá hacer constar cuantas observaciones estime convenientes. Se entregará copia del acta a la persona o representante de la entidad fiscalizada, dejando constancia, en su caso, de su negativa a firmarla o a estar presente en el desarrollo de la inspección.

En el ejercicio de las funciones de inspección el personal de la Comisión Nacional del Juego tendrá la condición de autoridad. El ejercicio de las facultades de inspección y control podrá ser objeto de convenio con las Comunidades Autónomas respecto de las actividades y de los medios o instrumentos situados en su territorio, con excepción de las de carácter resolutorio.

La Comisión Nacional del Juego colaborará con otros organismos reguladores del Espacio Económico Europeo en la persecución del juego ilegal, mediante la adopción de

medidas coordinadas para obtener la cesación en la prestación de servicios ilegales de juego y el intercambio de información.

5. La Comisión Nacional del Juego podrá firmar acuerdos de corregulación que coadyuven al cumplimiento de las obligaciones establecidas en esta Ley, en particular en lo referido a la publicidad, en los términos que se determinen reglamentariamente. En la medida en que dichos acuerdos afecten a la publicidad efectuada por los prestadores del servicio de comunicación audiovisual, deberá recabarse informe del Consejo Estatal de Medios Audiovisuales con carácter previo a la firma de los mismos. Los sistemas de autorregulación se dotarán de órganos independientes de control para asegurar el cumplimiento eficaz de los compromisos asumidos por las empresas adheridas. Sus códigos de conducta podrán incluir, entre otras, medidas individuales o colectivas de autocontrol previo de los contenidos publicitarios y deberán establecer sistemas eficaces de resolución extrajudicial de reclamaciones que cumplan los requisitos establecidos en la normativa comunitaria y, como tales, sean notificados a la Comisión Europea, de conformidad con lo previsto en la Resolución del Consejo de 25 de mayo de 2000 relativo a la red comunitaria de órganos nacionales de solución extrajudicial de litigios en materia de consumo o cualquier disposición equivalente.

6. La autoridad encargada de la regulación del juego podrá tener acceso a los datos de identidad tratados por las federaciones deportivas españolas y que sean necesarios para controlar el cumplimiento de las prohibiciones subjetivas previstas en las letras d), e) y f) del artículo 6.2.

[. . .]

Información relacionada

- Téngase en cuenta que, según establece la disposición adicional segunda, apartado 3, de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, Ref. BOE-A-2013-5940, las referencias contenidas en cualquier norma del ordenamiento jurídico a la Comisión Nacional del Juego se entenderán realizadas a la Dirección General de Ordenación del Juego del Ministerio de Consumo, que la sustituye y asume sus competencias, en los términos previstos en la disposición adicional décima de la citada Ley. Ref. BOE-A-2013-5940

§ 56

Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 318, de 31 de diciembre de 2010
Última modificación: 23 de enero de 2025
Referencia: BOE-A-2010-20139

[. . .]

TÍTULO II

Derechos de los usuarios de los servicios postales

[. . .]

Artículo 7. *Protección de datos.*

1. Conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, los operadores que presten servicios postales no podrían facilitar ningún dato relativo a la existencia del envío postal, a su clase, a sus circunstancias exteriores, a la identidad del remitente y del destinatario, ni a sus direcciones.

2. La obligación de protección de los datos incluirá el deber de secreto de los de carácter personal, la confidencialidad de la información transmitida o almacenada y la protección de la intimidad.

[. . .]

TÍTULO V

Acceso a la red postal de los operadores y resolución de conflictos entre ellos

CAPÍTULO I

Acceso a la red postal y a otras infraestructuras postales

[. . .]

Artículo 47. *Acceso a otras infraestructuras.*

Reglamentariamente se determinarán las condiciones de acceso de los titulares de autorizaciones administrativas singulares de manera transparente y no discriminatoria a otras infraestructuras postales tales como son el sistema de código postal, la base de datos de direcciones, los apartados postales, los buzones de distribución, la información sobre cambios de dirección, el servicio de reexpedición o el servicio de devolución al remitente,

siempre que ello resulte necesario para proteger el interés de los usuarios o favorecer una competencia real, según modalidades técnicas y tarifarias previstas en los acuerdos firmados a este fin con el operador designado, todo ello sin perjuicio de lo dispuesto en la normativa sobre protección de datos.

La Comisión Nacional del Sector Postal velará por la observancia de los principios de transparencia y no discriminación en dicho acceso.

[. . .]

Artículo 62. *Sanciones.*

1. Las infracciones leves se sancionarán con multa de 200 a 8.000 euros, las graves con multa de 8.001 a 80.000 euros y las muy graves con multa de 80.001 a 400.000 euros.

2. Las infracciones muy graves, en atención a las circunstancias que concurran en su comisión, podrán dar lugar a la revocación de la autorización administrativa singular para la prestación del servicio por el infractor. Asimismo podrán llevar aparejado el precintado, la incautación de los equipos o vehículos o la clausura de las instalaciones, hasta tanto no se disponga de la oportuna autorización administrativa.

3. La sanción firme por la infracción tipificada en el artículo 59.e) llevará aparejada, desde que se produzca, la inhabilitación del infractor para el ejercicio de la actividad postal por el plazo de un año.

4. Las cuantías señaladas en este artículo podrán ser actualizadas por la ley de presupuestos generales del Estado.

5. El importe de la sanción firme impuesta al operador postal, de acuerdo con la legislación de protección de datos de carácter personal por hechos que sean a su vez constitutivos de infracción postal, se descontará de la sanción de esta naturaleza que corresponda, con el límite del 50 por ciento de ella.

[. . .]

Disposición final segunda. *Puesta en funcionamiento del censo promocional.*

La Comisión Nacional del Sector Postal, en colaboración con los organismos competentes, en el plazo de un año desde la entrada en vigor de la presente ley, adoptará las medidas necesarias para garantizar el efectivo funcionamiento del censo promocional a que se refiere el artículo 31 de la Ley Orgánica de Protección de Datos.

[. . .]

§ 57

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 103, de 29 de abril de 2010
Última modificación: 23 de enero de 2025
Referencia: BOE-A-2010-6737

[. . .]

CAPÍTULO II

De la diligencia debida

[. . .]

Sección 3.ª Medidas reforzadas de diligencia debida

[. . .]

Artículo 15. *Tratamiento de datos de personas con responsabilidad pública.*

1. A fin de dar cumplimiento a las medidas establecidas en el artículo anterior, los sujetos obligados podrán proceder a la creación de ficheros donde se contengan los datos identificativos de las personas con responsabilidad pública, aun cuando no mantuvieran con las mismas una relación de negocios.

A tal efecto los sujetos obligados podrán recabar la información disponible acerca de las personas con responsabilidad pública sin contar con el consentimiento del interesado, aun cuando dicha información no se encuentre disponible en fuentes accesibles al público.

Los datos contenidos en los ficheros creados por los sujetos obligados únicamente podrán ser utilizados para el cumplimiento de las medidas reforzadas de diligencia debida previstas en esta Ley.

2. Será igualmente posible la creación por terceros distintos de los sujetos obligados de ficheros en los que se incluyan los datos identificativos de quienes tengan la condición de personas con responsabilidad pública con la exclusiva finalidad de colaborar con los sujetos obligados en el cumplimiento de las medidas reforzadas de diligencia debida.

Quienes procedan a la creación de estos ficheros no podrán emplear los datos para ninguna otra finalidad distinta de la señalada en el párrafo anterior.

3. El tratamiento y cesión de los datos a los que se refieren los dos apartados anteriores quedarán sujetos a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, en adelante, “Reglamento (UE) 2016/679, de 27 de abril de 2016’’ y en la Ley Orgánica 3/2018,

de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante, "Ley Orgánica 3/2018, de 5 de diciembre".

No obstante, no será preciso informar a los afectados acerca de la inclusión de sus datos en los ficheros a los que se refiere este artículo.

4. Los sujetos obligados y los terceros a que se refiere el apartado 2 deberán establecer procedimientos que permitan la actualización continua de los datos contenidos en los ficheros relativos a las personas con responsabilidad pública. En todo caso deberán aplicarse las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

[. . .]

CAPÍTULO III

De las obligaciones de información

[. . .]

Artículo 24. *Prohibición de revelación.*

1. Los sujetos obligados y sus directivos o empleados no revelarán al cliente ni a terceros que se ha comunicado información al Servicio Ejecutivo de la Comisión, o que se está examinando o puede examinarse alguna operación por si pudiera estar relacionada con el blanqueo de capitales o con la financiación del terrorismo.

Esta prohibición no incluirá la revelación a las autoridades competentes, incluidos los órganos centralizados de prevención, o la revelación por motivos policiales en el marco de una investigación penal.

2. La prohibición establecida en el apartado precedente no impedirá:

a) La comunicación de información entre sujetos obligados que pertenezcan al mismo grupo. A estos efectos, se estará a la definición de grupo establecida en el artículo 42 del Código de Comercio. Esta excepción es aplicable a la comunicación de información con sujetos obligados domiciliados en terceros países, siempre que se aplique en ellos políticas y procedimientos de grupo que cumplan con los requisitos establecidos en esta ley.

b) La comunicación de información entre los sujetos obligados a que se refieren los párrafos m) y ñ) del artículo 2.1, cuando ejerzan sus actividades profesionales, ya sea como empleados o de otro modo, dentro de la misma entidad jurídica o en una red. Se entenderá por red, a estos efectos, la estructura más amplia a la que pertenece la persona y que comparte una propiedad, gestión o supervisión de cumplimiento comunes.

c) La comunicación de información, referida a un mismo cliente y a una misma operación en la que intervengan dos o más entidades o personas, entre entidades financieras o entre los sujetos obligados a que se refieren los párrafos m) y ñ) del artículo 2.1, siempre que pertenezcan a la misma categoría profesional y estén sujetos a obligaciones equivalentes en lo relativo al secreto profesional y a la protección de datos personales. La información intercambiada se utilizará exclusivamente a efectos de la prevención del blanqueo de capitales y de la financiación del terrorismo.

Las excepciones establecidas en las letras anteriores también serán aplicables a la comunicación de información entre personas o entidades domiciliadas en la Unión Europea o en países terceros equivalentes.

Queda prohibida la comunicación de información con personas o entidades domiciliadas en países terceros no calificados como equivalentes o respecto de los que la Comisión Europea adopte la decisión a que se refiere la Disposición adicional de esta Ley.

3. Cuando los sujetos obligados a que se refieren las letras m) y ñ) del artículo 2.1 intenten disuadir a un cliente de una actividad ilegal, ello no constituirá revelación a efectos de lo dispuesto en el apartado primero.

[. . .]

CAPÍTULO IV

Del control interno

[. . .]

Artículo 26 bis. *Procedimientos internos de comunicación de potenciales incumplimientos.*

1. Los sujetos obligados establecerán procedimientos internos para que sus empleados, directivos o agentes puedan comunicar, incluso anónimamente, información relevante sobre posibles incumplimientos de esta ley, su normativa de desarrollo o las políticas y procedimientos implantados para darles cumplimiento, cometidos en el seno del sujeto obligado.

Estos procedimientos podrán integrarse en los sistemas que hubiera podido establecer el sujeto obligado para la comunicación de informaciones relativas a la comisión de actos o conductas que pudieran resultar contrarios a la restante normativa general o sectorial que les fuere aplicable.

2. Será de aplicación a estos sistemas y procedimientos lo dispuesto en la normativa de protección de datos de carácter personal para los sistemas de información de denuncias internas.

A estos efectos, se considerarán como órganos de control interno y cumplimiento exclusivamente los regulados en el artículo 26 ter.

3. Los sujetos obligados adoptarán medidas para garantizar que los empleados, directivos o agentes que informen de las infracciones cometidas en la entidad sean protegidos frente a represalias, discriminaciones y cualquier otro tipo de trato injusto.

4. La obligación de establecimiento del procedimiento de comunicación descrito en los apartados anteriores, no sustituye la necesaria existencia de mecanismos específicos e independientes de comunicación interna de operaciones sospechosas de estar vinculadas con el blanqueo de capitales o la financiación del terrorismo por parte de empleados a las que se refiere el artículo 18.

5. Reglamentariamente podrán determinarse los sujetos obligados exceptuados del cumplimiento de la obligación prevista en este artículo.

Artículo 26 ter. *Órgano de control interno y representante ante el Servicio Ejecutivo.*

1. Los sujetos obligados designarán como representante ante el Servicio Ejecutivo de la Comisión a una persona residente en España que ejerza cargo de administración o dirección de la sociedad.

En los grupos que integren varios sujetos obligados, el representante será único y deberá ejercer cargo de administración o dirección de la sociedad dominante del grupo.

En el caso de empresarios o profesionales individuales será representante ante el Servicio Ejecutivo de la Comisión el titular de la actividad.

2. Con las excepciones que se determinen reglamentariamente, la propuesta de nombramiento del representante, acompañada de una descripción detallada de su trayectoria profesional, será comunicada al Servicio Ejecutivo de la Comisión que, de forma razonada, podrá formular reparos u observaciones.

El representante ante el Servicio Ejecutivo de la Comisión será responsable del cumplimiento de las obligaciones de información establecidas en la presente ley, para lo que tendrá acceso sin limitación alguna a cualquier información obrante en el sujeto obligado así como en cualquiera de las entidades del grupo, en su caso.

3. Los sujetos obligados cuya administración central se encuentre en otro Estado miembro de la Unión Europea y que operen en España mediante agentes u otras formas de establecimiento permanente distintas de la sucursal deberán nombrar un representante residente en España, que tendrá la consideración de punto central de contacto.

Los sujetos obligados que operen en España en régimen de libre prestación de servicios deberán asimismo designar un representante ante el Servicio Ejecutivo de la Comisión, sin que sea exigible su residencia en España.

4. Los sujetos obligados establecerán un órgano adecuado de control interno responsable de la aplicación de las políticas y procedimientos a que se refiere el artículo 26.

El órgano de control interno, que contará, en su caso, con representación de las distintas áreas de negocio del sujeto obligado, se reunirá, levantando acta expresa de los acuerdos adoptados, con la periodicidad que se determine en el procedimiento de control interno.

5. Para el ejercicio de sus funciones el representante ante el Servicio Ejecutivo de la Comisión y el órgano de control interno deberán contar con los recursos materiales, humanos y técnicos necesarios.

6. Los órganos de prevención del blanqueo de capitales y la financiación del terrorismo operarán, en todo caso, con separación funcional del departamento o unidad de auditoría interna del sujeto obligado.

7. Reglamentariamente se determinarán las categorías de sujetos obligados que puedan exceptuarse de la obligación de constitución de un órgano de control interno, siendo las funciones de éste ejercidas en tales supuestos por el representante ante el Servicio Ejecutivo de la Comisión.

La norma reglamentaria determinará también las categorías de sujetos obligados para los que sea exigible la constitución de unidades técnicas para el tratamiento y análisis de la información.

[. . .]

Artículo 32. *Protección de datos de carácter personal.*

1. El tratamiento de datos personales para el cumplimiento de las obligaciones establecidas en el capítulo III de esta ley se encuentra amparado por lo dispuesto en el artículo 8.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y en el artículo 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, no precisando del consentimiento del interesado.

Tampoco será necesario el consentimiento para las comunicaciones de datos previstas en el citado capítulo y, en particular, para las previstas en el artículo 24.2, quedando igualmente amparadas por el artículo 8.1 de la Ley Orgánica 3/2018, de 5 de diciembre.

2. En virtud de lo dispuesto en el artículo 24.1, y de conformidad con el artículo 14.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, no será de aplicación al tratamiento de datos la obligación de información prevista en el artículo 14 del mencionado Reglamento en relación con los tratamientos a los que se refiere el apartado anterior.

Asimismo, de conformidad con el artículo 23 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, no procederá la atención de los derechos establecidos en los artículos 15 a 22 del Reglamento en relación con los citados tratamientos. En caso de ejercicio de los citados derechos por el interesado, los sujetos obligados se limitarán a ponerle de manifiesto lo dispuesto en este artículo.

Lo dispuesto en el presente apartado será igualmente aplicable a los tratamientos llevados a cabo por el Servicio Ejecutivo de la Comisión para el cumplimiento de las funciones que le otorga esta ley.

3. Los órganos centralizados de prevención a los que se refiere el artículo 27 tendrán la condición de encargados del tratamiento a los efectos previstos en la normativa de protección de datos personales.

Se exceptúan de lo señalado en el párrafo anterior los tratamientos que llevasen a cabo los órganos centralizados de prevención de incorporación obligatoria en el ámbito de las funciones que se les atribuyan reglamentariamente. La norma reglamentaria especificará los supuestos en que estos órganos tengan la condición de responsables del tratamiento.

4. Los sujetos obligados deberán realizar una evaluación de impacto en la protección de datos de los tratamientos a los que se refiere este artículo a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales. Dichas medidas deberán en todo caso garantizar la trazabilidad de los accesos y comunicaciones de los datos.

En todo caso, el tratamiento deberá llevarse únicamente a cabo por los órganos a los que se refiere el artículo 26 ter de esta ley.

5. Serán de aplicación a los ficheros creados en aplicación de lo dispuesto en el capítulo III las medidas de seguridad y control reforzadas.

Artículo 32 bis. *Protección de datos en el cumplimiento de las obligaciones de diligencia debida.*

1. El tratamiento de datos personales que resulte necesario para el cumplimiento de las obligaciones establecidas en el Capítulo II de esta ley se encuentra amparado por lo dispuesto en el artículo 8.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 6.1 c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, no precisando del consentimiento del interesado.

2. Los datos recogidos por los sujetos obligados para el cumplimiento de las obligaciones de diligencia debida no podrán ser utilizados para fines distintos de los relacionados con la prevención del blanqueo de capitales y la financiación del terrorismo sin el consentimiento del interesado, salvo que el tratamiento de dichos datos sea necesario para la gestión ordinaria de la relación de negocios.

3. Con carácter previo al establecimiento de la relación de negocios o la realización de una transacción ocasional, los sujetos obligados deberán facilitar a los nuevos clientes la información requerida en los artículos 13 y 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y en el artículo 11 de la Ley Orgánica 3/2018, de 5 de diciembre. Dicha información contendrá, en particular, un aviso general sobre las obligaciones legales de los sujetos obligados con respecto al tratamiento de datos personales a efectos de prevención del blanqueo de capitales y la financiación del terrorismo.

4. Los sujetos obligados deberán realizar una evaluación de impacto en la protección de datos de los tratamientos a los que se refiere este artículo a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales. Dichas medidas deberán en todo caso garantizar la trazabilidad de los accesos y comunicaciones de los datos.

Artículo 32 ter.

1. Los sujetos obligados pertenecientes a una misma categoría de las establecidas en el artículo 2 de esta ley podrán crear sistemas comunes de información, almacenamiento y, en su caso, acceso a la información y documentación recopilada para el cumplimiento de las obligaciones de diligencia debida establecidas en el capítulo II, con excepción de la relacionada con el seguimiento continuo de la relación de negocios, regulada en el artículo 6.

Los sujetos adheridos al sistema tendrán la condición de corresponsables del tratamiento a los efectos previstos en el artículo 26 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en el artículo 29 de la Ley Orgánica 3/2018, de 5 de diciembre.

El mantenimiento de estos sistemas podrá encomendarse a un tercero, aun cuando no tenga la condición de sujeto obligado.

Los sujetos obligados corresponsables deberán comunicar a la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias la intención de constituir estos sistemas al menos sesenta días antes de su puesta en funcionamiento. Esta comunicación no exime a las entidades financieras del cumplimiento de las obligaciones de notificación a que estén sujetas.

2. La comunicación de datos a los sistemas, así como el acceso a los datos incorporados a los mismos se encuentran amparados en lo dispuesto en el artículo 6.1.c) del Reglamento (UE) 2016/679, de 27 de abril de 2016, y en el artículo 8.1 de la Ley Orgánica 3/2018, de 5 de diciembre.

Los sujetos obligados solo podrán acceder a la información facilitada por otro sujeto obligado en los supuestos en que la persona a la que se refieran los datos sea su cliente o el acceso a la información sea necesario para el cumplimiento de las obligaciones de identificación previas al establecimiento de la relación de negocios previstas en el artículo 3. En este supuesto, solo se accederá a los datos necesarios a tal efecto.

3. Los datos serán facilitados al sistema por los órganos de control interno previstos en el artículo 26 ter. Estos órganos canalizarán asimismo las solicitudes de acceso a los datos contenidos en el sistema.

En todo caso, los interesados deberán ser informados acerca de la comunicación de los datos al sistema, así como del acceso que pretendiese llevarse a cabo con carácter previo a que el mismo se produzca.

4. Los datos obtenidos como consecuencia del acceso al sistema únicamente podrán ser empleados para el cumplimiento por los sujetos obligados de lo dispuesto en el capítulo II de esta ley.

5. Corresponderá al sujeto obligado que hubiera proporcionado los datos al sistema responder de su exactitud y actualización, debiendo cumplir en su caso lo establecido en los artículos 17.2 y 19 del Reglamento (UE) 2016/679, de 27 de abril de 2016. Conforme al artículo 26.3 del Reglamento (UE) 2016/679, los interesados podrán ejercer los derechos que les reconoce el citado Reglamento frente a, y en contra de, cada uno de los responsables.

Cuando el sujeto obligado compruebe, a la vista de la información que él mismo hubiese recabado en cumplimiento de sus deberes de diligencia debida, que los datos a los que hubiese accedido son incorrectos o no están actualizados, lo comunicará al sistema a fin de que los datos sean objeto de actualización o rectificación en su caso.

Del mismo modo deberá proceder cuando aprecie que un documento incorporado al sistema deba ser sustituido por otro más reciente.

6. Sin perjuicio de las restantes medidas que deban adoptarse en cumplimiento de lo dispuesto en el capítulo V del Reglamento (UE) 2016/679, de 27 de abril de 2016, y el título VI de la Ley Orgánica 3/2018, de 5 de diciembre, el sistema de información incorporará medidas que garanticen la trazabilidad de los accesos al mismo.

7. La Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias podrá autorizar el establecimiento de sistemas comunes en que participen varias categorías de sujetos obligados, delimitando dichas categorías y la información que podrá ser compartida.

Artículo 33. *Intercambio de información entre sujetos obligados y ficheros centralizados de prevención del fraude.*

1. Sin perjuicio de lo establecido en el artículo 24.2, cuando concurran riesgos extraordinarios identificados mediante los análisis de riesgos en materia de blanqueo de capitales y financiación del terrorismo llevados a cabo por los sujetos obligados, o a través de la actividad de análisis e inteligencia financieros del Servicio Ejecutivo de la Comisión, o del análisis de riesgo nacional en materia de blanqueo de capitales y de la financiación del terrorismo, la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, previo dictamen conforme de la Agencia Española de Protección de Datos, podrá acordar el intercambio de información referida a determinado tipo de operaciones distintas de las previstas en los artículos 18 y 19 o a clientes sujetos a determinadas circunstancias siempre que el mismo se produzca entre sujetos obligados que se encuentren en una o varias de las categorías previstas en el artículo 2.

El Acuerdo determinará en todo caso el tipo de operación o la categoría de cliente respecto de la que se autoriza el intercambio de información, así como las categorías de sujetos obligados que podrán intercambiar la información.

2. Asimismo, los sujetos obligados podrán intercambiar información relativa a las operaciones a las que se refiere el artículo 18 con la única finalidad de prevenir o impedir operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo cuando de las características u operativa del supuesto concreto se desprenda la posibilidad de que, una vez rechazada, pueda intentarse ante otros sujetos obligados el desarrollo de una operativa total o parcialmente similar a aquélla.

Quedarán excluidas aquellas operaciones que hayan sido objeto de devolución por el Servicio Ejecutivo de la Comisión, conforme al artículo 18.2.

3. El tratamiento de los datos personales al que se refieren los dos apartados anteriores, cuando proceda, se encontrará amparado en lo dispuesto en el artículo 8.2 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 6.1 e) del Reglamento (UE) 2016/679

del Parlamento Europeo y del Consejo, de 27 de abril de 2016, no siendo preciso contar con el consentimiento del interesado.

4. De acuerdo con el artículo 24.1, y de conformidad con el artículo 14.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, no será de aplicación al tratamiento de datos la obligación de información prevista en el artículo 14 del Reglamento en relación con los tratamientos a los que se refieren los apartados 1 y 2.

Asimismo, de conformidad con el artículo 23 del Reglamento (UE) 2016/679, no procederá la atención de los derechos establecidos en los artículos 15 a 22 del Reglamento en relación con los citados tratamientos. En caso de ejercicio de los citados derechos por el interesado, los sujetos obligados se limitarán a ponerle de manifiesto lo dispuesto en este artículo.

5. Los sujetos obligados o quienes desarrollen los sistemas que sirvan de soporte al intercambio de información al que se refieren los apartados 1 y 2 deberán realizar una evaluación de impacto en la protección de datos de los citados tratamientos a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales. Dichas medidas deberán en todo caso garantizar la trazabilidad de los accesos y comunicaciones de los datos.

El acceso a los datos quedará limitado a los órganos de control interno previstos en el artículo 26 ter, con inclusión de las unidades técnicas que constituyan los sujetos obligados.

6. Los sujetos obligados y las autoridades judiciales, policiales y administrativas competentes en materia de prevención o represión del blanqueo de capitales o de la financiación del terrorismo podrán consultar la información contenida en los sistemas que fueren creados, de acuerdo con lo previsto en la normativa vigente en materia de protección de datos personales, siempre que el acceso a dicha información fuere necesario para las finalidades descritas en los apartados anteriores.

[. . .]

CAPÍTULO VI

Otras disposiciones

[. . .]

Artículo 43. *Fichero de Titularidades Financieras.*

1. Con la finalidad de prevenir, impedir y detectar el blanqueo de capitales y la financiación del terrorismo, así como para fines de prevención, detección, investigación o enjuiciamiento de delitos graves, las entidades de crédito, las entidades de dinero electrónico y las entidades de pago (en adelante, las entidades declarantes) deberán declarar al Servicio Ejecutivo de la Comisión, con la periodicidad que reglamentariamente se determine, la apertura o cancelación de cuentas corrientes, cuentas de ahorro, depósitos y de cualquier otro tipo de cuentas de pago, así como los contratos de alquiler de cajas de seguridad y su periodo de arrendamiento, con independencia de su denominación comercial.

Las declaraciones no incluirán las cajas de seguridad, cuentas y depósitos de las sucursales o filiales de las entidades declarantes españolas en el extranjero.

La declaración contendrá, en todo caso, los datos identificativos de los titulares y de sus titulares reales y los datos identificativos de los representantes o autorizados y cualesquiera otras personas con poderes de disposición. La información de los productos a declarar incluirá en todo caso la numeración que los identifique, el tipo de producto declarado y las fechas de apertura y de cancelación. En el caso de las cajas de seguridad se incluirá la duración del periodo de arrendamiento. Reglamentariamente se podrán determinar otros datos de identificación que deban ser declarados.

2. Los datos declarados serán incluidos en un fichero de titularidad pública, denominado Fichero de Titularidades Financieras, del cual será responsable la Secretaría de Estado de Economía y Apoyo a la Empresa.

El Servicio Ejecutivo de la Comisión, como encargado del tratamiento, determinará, con arreglo a lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, y en el Reglamento

(UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, las características técnicas del fichero, pudiendo aprobar las instrucciones pertinentes.

El tratamiento de los datos personales contenidos en el Fichero de Titularidades Financieras por el Servicio Ejecutivo de la Comisión se regirá por lo establecido en el artículo 28.3 del Reglamento (UE) 2016/679, de 27 de abril de 2016. El Servicio Ejecutivo de la Comisión podrá utilizar la información obrante en el mismo para el ejercicio de sus competencias.

3. Con ocasión de la investigación de delitos relacionados con el blanqueo de capitales o la financiación del terrorismo, podrán acceder al Fichero de Titularidades Financieras los órganos jurisdiccionales con competencias en la investigación de estos delitos, el Ministerio Fiscal y la Fiscalía Europea en el ejercicio de sus competencias, así como:

Las Fuerzas y Cuerpos de Seguridad del Estado y las Policías Autonómicas con competencias estatutariamente asumidas para la investigación de los delitos graves.

Los organismos de recuperación de activos, incluida la Oficina de Recuperación y Gestión de Activos, podrán acceder al Fichero cuando les haya sido encomendada la localización de activos por los órganos judiciales o fiscalías, así como en la realización de sus funciones de intercambio de información con otras oficinas análogas de la Unión Europea o instituciones de terceros Estados cuyo fin sea el embargo o decomiso en el marco de un procedimiento penal y se trate de delitos relacionados con el blanqueo de capitales o la financiación del terrorismo.

La Secretaría de la Comisión de Vigilancia de Actividades de Financiación del Terrorismo podrá acceder al Fichero en el marco de las competencias que tiene atribuidas en materia de bloqueo de los saldos, cuentas y posiciones, incluidos los bienes depositados en cajas de seguridad abiertas por personas o entidades vinculadas a organizaciones terroristas, en virtud de los artículos 1 y 2 de la Ley 12/2003, de 21 de mayo, de prevención y bloqueo de la financiación del terrorismo, y del Reglamento de la Comisión de Vigilancia de Actividades de Financiación del Terrorismo, aprobado por el Real Decreto 413/2015, de 29 de mayo.

El Centro Nacional de Inteligencia podrá acceder a los datos declarados en el Fichero de Titularidades Financieras para el cumplimiento de las funciones que tiene asignadas en su normativa reguladora.

La Agencia Estatal de Administración Tributaria podrá acceder al Fichero de Titularidades Financieras para el ejercicio de sus competencias en materia de prevención y lucha contra el fraude, en los términos previstos en la Ley 58/2003, de 17 de diciembre, General Tributaria, y en el artículo 7.3 bis del Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo, de 11 de septiembre de 2013, relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude. Igual acceso dispondrán las Haciendas Forales para la mencionada finalidad.

Toda petición de acceso a los datos del Fichero de Titularidades Financieras habrá de realizarse a través de los respectivos puntos únicos de acceso que deberán asignarse a todas las autoridades anteriormente señaladas y deberá ser adecuadamente motivada por el órgano requirente, que será responsable de la regularidad del requerimiento. En ningún caso podrá requerirse el acceso al Fichero para finalidades distintas de las previstas en este artículo. Los accesos quedarán registrados y los datos de los registros se conservarán por un plazo de 5 años.

4. Sin perjuicio de las competencias que correspondan a la Agencia Española de Protección de Datos y al Consejo General del Poder Judicial en relación con los tratamientos con fines jurisdiccionales realizados por los órganos judiciales, un miembro del Ministerio Fiscal designado por el Fiscal General del Estado, de conformidad con los trámites previstos en el Estatuto Orgánico del Ministerio Fiscal, y que durante el ejercicio de esta actividad no se encuentre desarrollando su función en alguno de los órganos del Ministerio Fiscal encargados de la persecución de los delitos de blanqueo de capitales o financiación del terrorismo, velará por el uso adecuado del fichero, a cuyos efectos podrá requerir, con posterioridad a cualquier acceso, justificación completa de los motivos del mismo.

[. . .]

Artículo 48 bis. *Cooperación internacional.*

1. La Secretaría de la Comisión, el Servicio Ejecutivo de la Comisión o, en caso de convenio, el Banco de España, la Comisión Nacional del Mercado de Valores y la Dirección General de Seguros y Fondos de Pensiones, cooperarán por propia iniciativa o previa solicitud, en tiempo oportuno y gratuitamente, con otras autoridades competentes de la Unión Europea siempre que sea necesario para llevar a cabo las funciones establecidas en esta ley, haciendo uso, a tal fin, de todas las facultades que la misma les atribuye y sin imponer condiciones indebidamente restrictivas. En el marco de esta cooperación se facilitará a la Autoridad Bancaria Europea la información necesaria para permitirle llevar a cabo sus obligaciones en materia de prevención del blanqueo de capitales y de la financiación del terrorismo. Este intercambio de información estará sometido al deber de secreto profesional previsto en el artículo 49.1 de la ley.

2. En el caso de autoridades competentes de terceros países no miembros de la Unión Europea, la cooperación e intercambio de información se condicionará a lo dispuesto en los Convenios y Tratados Internacionales o, en su caso, al principio general de reciprocidad, así como al sometimiento de dichas autoridades extranjeras a las mismas obligaciones de secreto profesional que rigen para las españolas.

3. El intercambio de información del Servicio Ejecutivo de la Comisión con Unidades de Inteligencia Financiera de Estados de la Unión Europea se realizará de conformidad con lo dispuesto en los artículos 51 a 57 de la Directiva 2015/849, del Parlamento Europeo y del Consejo, de 20 de mayo de 2015 relativa a la prevención de la utilización del sistema financiero para la prevención del blanqueo de capitales o la financiación del terrorismo.

4. El intercambio de información del Servicio Ejecutivo de la Comisión con Unidades de Inteligencia Financiera de terceros países no miembros de la Unión Europea se realizará de acuerdo con los principios del Grupo Egmont o en los términos del correspondiente memorando de entendimiento. Los memorandos de entendimiento con Unidades de Inteligencia Financiera serán suscritos por el Director del Servicio Ejecutivo, previa autorización de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, debiendo contar con el previo informe favorable de la Agencia Española de Protección de Datos.

5. La Secretaría de la Comisión, el Servicio Ejecutivo de la Comisión o los órganos supervisores a que se refiere el artículo 44 podrán utilizar la información recibida únicamente para los fines para los que las autoridades cedentes hayan dado su consentimiento. Esta información no será transmitida a otros organismos o personas físicas y jurídicas sin el consentimiento expreso de las autoridades competentes que la hayan divulgado.

6. A requerimiento de la Unidad de Inteligencia Financiera de otro Estado miembro de la Unión Europea, el Servicio Ejecutivo de la Comisión estará facultado para suspender una transacción en curso, cuando concurran indicios de blanqueo de capitales o financiación del terrorismo a fin de que por parte de la Unidad de Inteligencia Financiera requirente se proceda a analizar la transacción, confirmar la sospecha y comunicar los resultados del análisis a las autoridades competentes. En los casos de suspensión por indicios de financiación de terrorismo, informará a la Secretaría de la Comisión de Vigilancia de Actividades de Financiación del Terrorismo cuando exista la previa autorización de la Unidad de Inteligencia Financiera requirente.

La suspensión se acordará bajo la responsabilidad de la Unidad de Inteligencia Financiera requirente y será efectiva por un periodo máximo de un mes. Transcurrido dicho plazo, cesará la suspensión salvo que fuera ratificada o prorrogada judicialmente a solicitud del Ministerio Fiscal.

[. . .]

Artículo 63. *Comunicación de infracciones.*

1. Los empleados, directivos y agentes de los sujetos obligados que conozcan hechos o situaciones que puedan ser constitutivos de infracciones contempladas en esta ley, los podrán poner en conocimiento del Servicio Ejecutivo de la Comisión.

2. Las comunicaciones serán remitidas al Servicio Ejecutivo de la Comisión por escrito e incorporarán todos los documentos e informaciones sobre los hechos denunciados que

permitan justificar la denuncia. Mediante orden del Ministro de Economía y Empresa se aprobará el modelo de comunicación y se establecerán las características y requisitos del canal de recepción de comunicaciones, a fin de asegurar su confidencialidad y seguridad.

3. Los programas de formación de las entidades deberán incluir la información sobre la existencia de estos mecanismos.

Artículo 64. *Tratamiento de las comunicaciones.*

1. El Servicio Ejecutivo de la Comisión determinará si existe o no sospecha fundada de infracción en las comunicaciones recibidas de conformidad con el artículo 63. De no existir sospecha fundada o cuando no se concreten suficientemente los hechos o personas responsables de la infracción, requerirá a la persona comunicante para que aclare el contenido de la comunicación realizada, o lo complemente con nueva información, concediendo un plazo para ello no inferior a 15 días. Transcurrido el plazo fijado para la aclaración o aportación de nueva información, sin que pueda determinarse sospecha fundada, se procederá al archivo de la comunicación.

2. Las comunicaciones recibidas no tendrán valor probatorio y no podrán ser incorporadas directamente al procedimiento administrativo. Si existen indicios suficientes de veracidad en los hechos imputados y éstos son desconocidos para la Administración, el Servicio Ejecutivo de la Comisión, o los supervisores de las entidades financieras, en caso de convenio de los previstos en el artículo 44. 2 m) de la ley, podrán:

a) Utilizar la información obtenida para la definición del nuevo plan de inspección.

b) Realizar actuaciones adicionales de inspección, que podrán llevarse a cabo de manera independiente o incardinarse en las acciones de supervisión planificadas en el contexto del desarrollo del plan anual de inspección aprobado.

3. Los resultados de las actuaciones de inspección llevadas a cabo por el Servicio Ejecutivo de la Comisión serán remitidas a la Secretaría de la Comisión, que las elevará a la consideración del Comité Permanente. Cuando las actuaciones de comprobación pongan de manifiesto la posible existencia de un ilícito penal, la información será remitida al Ministerio Fiscal para su investigación.

Artículo 65. *Protección de las personas.*

1. Las comunicaciones realizadas al amparo del artículo 63:

a) no constituirán violación o incumplimiento de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa que pudieran afectar a la persona comunicante, a las personas estrechamente vinculadas con ésta, a las sociedades que administre o de las que sea titular real;

b) no constituirán infracción de ningún tipo en el ámbito de la normativa laboral por parte de la persona comunicante, ni de ella podrá derivar trato injusto o discriminatorio por parte del empleador;

c) no generarán ningún derecho de compensación o indemnización a favor de la empresa a la que presta servicios la persona comunicante o de un tercero.

2. El Servicio Ejecutivo de la Comisión informará de los diferentes mecanismos legales que la normativa en vigor habilita para la garantía de estos derechos.

3. Las comunicaciones tendrán carácter confidencial, no pudiendo desvelar el Servicio Ejecutivo de la Comisión los datos identificativos de las personas que las hubieran realizado. En el caso de que, como consecuencia de la comunicación realizada, se inicie un expediente sancionador contra una persona física o jurídica, no se incluirán en ningún caso los datos de la persona que llevó a cabo la comunicación.

4. La comunicación realizada al amparo de lo previsto en el artículo 63 no conferirá por sí sola la condición de interesado en el procedimiento administrativo que pudiera iniciarse contra el infractor.

5. Las personas expuestas a amenazas, acciones hostiles o medidas laborales adversas por comunicar por vía interna o al Servicio Ejecutivo de la Comisión comunicaciones sobre actividades relacionadas con el blanqueo de capitales o la financiación del terrorismo podrán presentar una reclamación ante la Autoridad Independiente de Protección del Informante,

A.A.I. en los términos previstos en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

En los casos en los que el sujeto obligado no haya adoptado las medidas adecuadas para mantener la confidencialidad sobre la identidad de los empleados, directivos o agentes que hayan realizado una comunicación a los órganos de control interno, en los términos del artículo 30.1, será de aplicación el artículo 52.1.s).

[. . .]

§ 58

Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 55, de 4 de marzo de 2010
Última modificación: 1 de marzo de 2023
Referencia: BOE-A-2010-3514

[. . .]

TÍTULO I

Responsabilidad institucional en el ámbito de la salud, los derechos sexuales y reproductivos

[. . .]

CAPÍTULO IV

Medidas para la aplicación efectiva de la ley

[. . .]

Artículo 11 bis. *Investigación, recopilación y producción de datos.*

1. La investigación en materia de salud, derechos sexuales y reproductivos se garantizará a través de políticas públicas con enfoque de género e interseccional que permitan obtener la mejor, más amplia y actualizada información científica respecto de la salud sexual, la salud reproductiva, la salud durante la menstruación y la salud durante la menopausia y el climaterio en cada etapa correspondiente del ciclo vital.

2. Las administraciones públicas llevarán a cabo y apoyarán la realización de estudios, encuestas y trabajos de investigación sobre las temáticas reguladas por esta ley orgánica, así como aquellos otros que, integrando la perspectiva de género e interseccional, las tengan en cuenta, a fin de obtener y producir el mejor y más actualizado conocimiento que sea posible en el ámbito de la salud, los derechos sexuales y reproductivos. Se promoverá la recogida de datos y la elaboración de estudios sobre las infecciones de transmisión sexual, con la finalidad de analizar su prevalencia y guiar las medidas para su prevención y tratamiento. Asimismo, se promoverán los estudios sobre la crisis de reproducción y sus impactos sociales.

3. Se promoverá y garantizará la investigación que permita obtener la mejor, más amplia y actualizada información acerca de la menstruación y la salud durante la menstruación en las diferentes fases del ciclo vital de las mujeres, con un enfoque relativo a la prevención, diagnóstico y tratamiento de patologías que afectan al ciclo menstrual y los efectos que sobre este producen los distintos fármacos.

4. En la elaboración de las políticas públicas y en la realización de estudios, encuestas y trabajos de investigación se dará cumplimiento a la normativa vigente en materia de protección de datos de carácter personal.

5. Los objetivos de la investigación serán buscar soluciones a problemas específicos, explicar fenómenos y realidades, elaborar recomendaciones y propuestas de acción, desarrollar teorías, ampliar conocimientos, establecer principios y reformular planteamientos en relación con la promoción, protección y respeto de los derechos consagrados en esta ley orgánica.

TÍTULO II

De la interrupción voluntaria del embarazo

[. . .]

CAPÍTULO II

Garantías en el acceso a la prestación

[. . .]

Artículo 19 ter. *Registros de personas objetoras de conciencia.*

1. A efectos organizativos y para una adecuada gestión de la prestación se creará en cada comunidad autónoma y en el Instituto Nacional de Gestión Sanitaria (INGESA) un registro de personas profesionales sanitarias que decidan objetar por motivos de conciencia respecto de la intervención directa en la práctica de la interrupción voluntaria del embarazo.

2. Quienes se declaren personas objetoras de conciencia lo serán a los efectos de la práctica directa de la prestación de interrupción voluntaria del embarazo tanto en el ámbito de la sanidad pública como de la privada.

3. En el seno del Consejo Interterritorial del Sistema Nacional de Salud, se acordará un protocolo específico que incluya las condiciones mínimas para garantizar el cumplimiento de los objetivos perseguidos con la creación de este Registro, junto a la salvaguarda de la protección de datos de carácter personal, conforme a lo previsto en la disposición adicional cuarta.

4. Se adoptarán las medidas organizativas necesarias para garantizar la no discriminación tanto de las personas profesionales sanitarias no objetoras, evitando que se vean relegadas en exclusiva a la práctica de la interrupción voluntaria del embarazo, como de las personas objetoras para evitar que sufran cualquier discriminación derivada de la objeción.

Artículo 20. *Protección del derecho a la intimidad, a la confidencialidad y a la protección de datos.*

1. Los centros públicos y privados que presten cualquier tipo de asistencia sanitaria en relación con la salud sexual y reproductiva, y, en particular, la interrupción voluntaria del embarazo, garantizarán el derecho a la intimidad y a la confidencialidad de las pacientes en el tratamiento de sus datos de carácter personal.

2. De manera general, el tratamiento de datos de carácter personal y sanitario, así como el ejercicio de los derechos de la paciente, se ajustarán a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y a la Ley 41/2002, de 14 de noviembre.

3. Los centros prestadores del servicio deberán contar con sistemas de custodia activa y diligente de las historias clínicas de las pacientes e implantar en el tratamiento de los datos las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo conforme a la normativa vigente de protección de datos de carácter personal.

Artículo 21. *Tratamiento de datos.*

1. En el momento de la solicitud de información sobre la interrupción voluntaria del embarazo, los centros, sin proceder al tratamiento de dato alguno, habrán de informar a la solicitante que los datos identificativos de las pacientes a las que efectivamente se les realice la prestación serán objeto de codificación y separados de los datos de carácter clínico asistencial relacionados con la interrupción voluntaria del embarazo.

2. Los centros que presten la interrupción voluntaria del embarazo establecerán mecanismos apropiados de automatización y codificación de los datos de identificación de las pacientes atendidas, en los términos previstos en esta Ley.

A los efectos previstos en el párrafo anterior, se considerarán datos identificativos de la paciente su nombre, apellidos, domicilio, número de teléfono, dirección de correo electrónico, documento nacional de identidad o documento identificativo equivalente, así como cualquier dato que revele su identidad física o genética.

3. En el momento de la primera recogida de datos de la paciente, se le asignará un código que será utilizado para identificarla en todo el proceso.

4. Los centros sustituirán los datos identificativos de la paciente por el código asignado en cualquier información contenida en la historia clínica que guarde relación con la práctica de la interrupción voluntaria del embarazo, de forma que no pueda producirse con carácter general, el acceso a dicha información.

5. Las informaciones relacionadas con la interrupción voluntaria del embarazo deberán ser conservadas en la historia clínica de tal forma que su mera visualización no sea posible salvo por el personal que participe en la práctica de la prestación, sin perjuicio de los accesos a los que se refiere el artículo siguiente.

Artículo 22. *Acceso y cesión de datos de carácter personal.*

1. Únicamente será posible el acceso a los datos de la historia clínica asociados a los que identifican a la paciente, sin su consentimiento, en los casos previstos en las disposiciones legales reguladoras de los derechos y obligaciones en materia de documentación clínica.

Cuando el acceso fuera solicitado por otro profesional sanitario a fin de prestar la adecuada asistencia sanitaria de la paciente, aquél se limitará a los datos estricta y exclusivamente necesarios para la adecuada asistencia, quedando constancia de la realización del acceso.

En los demás supuestos amparados por la ley, el acceso se realizará mediante autorización expresa del órgano competente en la que se motivarán de forma detallada las causas que la justifican, quedando en todo caso limitado a los datos estricta y exclusivamente necesarios.

2. El informe de alta, las certificaciones médicas y cualquier otra documentación relacionada con la práctica de la interrupción voluntaria del embarazo que sea necesaria a cualquier efecto, será entregada exclusivamente a la paciente o persona autorizada por ella. Esta documentación respetará el derecho de la paciente a la intimidad y confidencialidad en el tratamiento de los datos de carácter personal recogido en este Capítulo.

3. No será posible el tratamiento de la información por el centro sanitario para actividades de publicidad o prospección comercial. No podrá recabarse el consentimiento de la paciente para el tratamiento de los datos para estas actividades.

Artículo 23. *Supresión de datos.*

1. Los centros que hayan procedido a una interrupción voluntaria de embarazo deberán suprimir de oficio la totalidad de los datos de la paciente que consten en sus registros administrativos una vez transcurridos cinco años desde la fecha de alta de la intervención. No obstante, la documentación clínica podrá conservarse cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud, en cuyo caso se procederá a la supresión de todos los datos identificativos de la paciente y del código que se le hubiera asignado como consecuencia de lo dispuesto en los artículos anteriores.

2. Lo dispuesto en el apartado anterior se entenderá sin perjuicio del ejercicio por la paciente de su derecho de supresión, en los términos previstos en el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre.

[. . .]

Disposición adicional cuarta. *Protección de datos de carácter personal en los Registros de personas objetoras de conciencia.*

1. Los datos personales que contengan los Registros de personas objetoras de conciencia regulados en el artículo 19 ter se llevarán a cabo conforme a lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. El fundamento jurídico de legitimación para el tratamiento de los datos que recoja el Registro de personas objetoras, de acuerdo con su objetivo y finalidad, se encuentra en las letras g) e i) del apartado 2 de los artículos 9 y concordantes del Reglamento General de Protección de Datos, así como en las letras c) y e) del apartado 1 de su artículo 6.

3. Los datos de las personas objetoras recogidos en cada uno de los Registros serán aquellos que resulten estrictamente necesarios para identificar al personal sanitario que desarrolle su actividad en centros sanitarios acreditados para la realización de la interrupción voluntaria del embarazo cuyas funciones conlleven su participación directa en las citadas intervenciones. Los datos objeto de tratamiento deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son recogidos, no debiendo incluirse, en ningún caso, el motivo de la objeción.

4. La finalidad perseguida con el tratamiento de los datos recabados en virtud del artículo 19 ter es la garantía de la prestación de la interrupción voluntaria del embarazo, adecuando los recursos humanos a la correcta programación de las intervenciones de interrupción voluntaria del embarazo. Los datos no podrán ser utilizados en ningún caso con fines distintos a los establecidos en este precepto.

5. Son responsables del tratamiento las Consejerías competentes en materia de sanidad de las comunidades autónomas y el Instituto Nacional de Gestión Sanitaria (INGESA), de acuerdo con sus respectivos ámbitos competenciales.

6. Las personas titulares de las Direcciones o Gerencias de los centros sanitarios acreditados para la realización de la interrupción voluntaria del embarazo tienen la consideración de destinatarias de los datos que sean estrictamente necesarios para la correcta planificación del servicio. Asimismo, tendrán esta condición respecto de los datos personales que sean estrictamente necesarios para conocer el número de personas objetoras en cada centro sanitario, acreditado quienes sean responsables de planificar los recursos humanos en cada Comunidad Autónoma y en el Instituto Nacional de Gestión Sanitaria (INGESA), con el fin de garantizar la prestación de la interrupción voluntaria del embarazo.

7. Las personas responsables y encargadas del tratamiento, así como todas las personas que intervengan en cualquier fase del mismo, estarán sujetas al deber de confidencialidad regulado por el artículo 5.1.f) del Reglamento general de protección de datos, sin perjuicio de los deberes de secreto profesional que, en su caso, resulten de aplicación.

8. La recolección de datos se hará conforme a la legislación vigente, con especial atención a:

a) La confidencialidad y la autenticidad de la identificación de la persona titular de los datos mediante certificado electrónico o instrumento similar de identificación segura.

b) El cumplimiento del deber de información previa a los interesados en los términos previstos en el artículo 13 del Reglamento general de protección de datos.

9. De acuerdo con la finalidad del tratamiento, se conservarán los datos recogidos durante el tiempo necesario para el cumplimiento del fin para el cual fueron recogidos y, en

su caso, podrán conservarse, debidamente bloqueados, por el tiempo necesario para atender a las responsabilidades derivadas de su tratamiento ante los órganos administrativos o jurisdiccionales competentes. Una vez trascurrido dicho periodo de conservación, los datos serán suprimidos definitivamente.

10. Las administraciones públicas que sean responsables del tratamiento deberán implementar la protección de datos desde el diseño, de acuerdo con lo previsto en el artículo 25 del Reglamento general de protección de datos, realizando, desde el momento de la concepción del tratamiento, el correspondiente análisis de riesgos y evaluación de impactos para determinar las medidas técnicas y organizativas adecuadas. Estas medidas garantizarán los derechos y libertades de la persona interesada, así como la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los accesos a los datos, teniendo en cuenta, en todo momento, lo previsto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

11. La persona titular de los datos podrá ejercer todos los derechos regulados en los artículos 13 a 22 del Reglamento General de Protección de Datos, excepto el de oposición, al basarse el tratamiento en el cumplimiento de una obligación legal, conforme al artículo 6.1.c) del Reglamento General de Protección de Datos.

[. . .]

§ 59

Ley 54/2007, de 28 de diciembre, de Adopción internacional. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 312, de 29 de diciembre de 2007
Última modificación: 22 de marzo de 2021
Referencia: BOE-A-2007-22438

TÍTULO I

Disposiciones generales

[. . .]

CAPÍTULO III

Capacidad y requisitos para la adopción internacional

[. . .]

Artículo 13. *Protección de datos de carácter personal.*

1. El tratamiento y la cesión de datos derivados del cumplimiento de las previsiones de la presente ley se encontrarán sometidos a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Los datos obtenidos por las Entidades Públicas o por los organismos acreditados únicamente podrán ser tratados para las finalidades relacionadas con el desarrollo, en cada caso, de las funciones descritas para cada una de ellas en los artículos 5 y 6.3 de la presente ley.

3. La transferencia internacional de los datos a autoridades extranjeras de adopción únicamente se efectuará en los supuestos expresamente previstos en esta ley y en el Convenio de La Haya, de 29 de mayo de 1993, relativo a la protección del niño y a la cooperación en materia de adopción internacional y demás legislación internacional.

[. . .]

§ 60

Ley Orgánica 11/2007, de 22 de octubre, reguladora de los derechos y deberes de los miembros de la Guardia Civil. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 254, de 23 de octubre de 2007
Última modificación: 29 de julio de 2015
Referencia: BOE-A-2007-18391

[. . .]

TÍTULO II

Del ejercicio de derechos fundamentales y libertades públicas

[. . .]

Artículo 5. *Derecho a la intimidad y a la vida privada.*

1. Los miembros de la Guardia Civil tienen garantizados los derechos a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones, en los términos establecidos en la Constitución y en el resto del ordenamiento jurídico.

A estos efectos el pabellón que tuviera asignado el Guardia Civil en su unidad se considerará domicilio habitual.

2. El jefe de la unidad, centro u órgano donde el Guardia Civil preste sus servicios podrá autorizar, de forma expresamente motivada, el registro personal o de los efectos y pertenencias que estuvieren en los mismos, cuando lo exija la investigación de un hecho delictivo. El registro se realizará con la asistencia del interesado y en presencia de, al menos, un testigo.

3. Los datos relativos a los miembros de la Guardia Civil estarán sujetos a la legislación sobre protección de datos de carácter personal.

[. . .]

§ 61

Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 242, de 9 de octubre de 2007
Última modificación: sin modificaciones
Referencia: BOE-A-2007-17634

[. . .]

Disposición Adicional Segunda. *Régimen jurídico.*

La presente Ley se inscribe en el marco de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la cual, por su propia naturaleza, resulta de aplicación directa, siendo los preceptos de esta Ley especificidades habilitadas por la citada Ley Orgánica en función de la naturaleza de la base de datos que se regula.

[. . .]

§ 62

Ley Orgánica 2/2006, de 3 de mayo, de Educación. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 106, de 4 de mayo de 2006
Última modificación: 8 de junio de 2024
Referencia: BOE-A-2006-7899

[. . .]

Disposición adicional vigesimotercera. *Datos personales de los alumnos.*

1. Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.

2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.

3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.

4. La cesión de los datos, incluidos los de carácter reservado, necesarios para el sistema educativo, se realizará preferentemente por vía telemática y estará sujeta a la legislación en materia de protección de datos de carácter personal. En el caso de la cesión de datos entre Comunidades Autónomas o entre éstas y el Estado, las condiciones mínimas serán acordadas por el Gobierno con las Comunidades Autónomas, en el seno de la Conferencia Sectorial de Educación.

[. . .]

§ 63

Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 313, de 29 de diciembre de 2004
Última modificación: 7 de septiembre de 2022
Referencia: BOE-A-2004-21760

[. . .]

TÍTULO V

Tutela Judicial

[. . .]

CAPÍTULO IV

Medidas judiciales de protección y de seguridad de las víctimas

[. . .]

Artículo 63. *De la protección de datos y las limitaciones a la publicidad.*

1. En las actuaciones y procedimientos relacionados con la violencia de género se protegerá la intimidad de las víctimas; en especial, sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia.

2. Los Jueces competentes podrán acordar, de oficio o a instancia de parte, que las vistas se desarrollen a puerta cerrada y que las actuaciones sean reservadas.

[. . .]

§ 64

Ley 58/2003, de 17 de diciembre, General Tributaria. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 302, de 18 de diciembre de 2003
Última modificación: 21 de diciembre de 2024
Referencia: BOE-A-2003-23186

[. . .]

TÍTULO III

La aplicación de los tributos

CAPÍTULO I

Principios generales

[. . .]

Sección 3.ª Colaboración social en la aplicación de los tributos

[. . .]

Artículo 94. *Autoridades sometidas al deber de informar y colaborar.*

1. Las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos del Estado, de las comunidades autónomas y de las entidades locales; los organismos autónomos y las entidades públicas empresariales; las cámaras y corporaciones, colegios y asociaciones profesionales; las mutualidades de previsión social; las demás entidades públicas, incluidas las gestoras de la Seguridad Social y quienes, en general, ejerzan funciones públicas, estarán obligados a suministrar a la Administración tributaria cuantos datos, informes y antecedentes con trascendencia tributaria recabe ésta mediante disposiciones de carácter general o a través de requerimientos concretos, y a prestarle, a ella y a sus agentes, apoyo, concurso, auxilio y protección para el ejercicio de sus funciones.

Asimismo, participarán en la gestión o exacción de los tributos mediante las advertencias, repercusiones y retenciones, documentales o pecuniarias, de acuerdo con lo previsto en las leyes o disposiciones reglamentarias vigentes.

2. A las mismas obligaciones quedarán sujetos los partidos políticos, sindicatos y asociaciones empresariales.

3. Los juzgados y tribunales deberán facilitar a la Administración tributaria, de oficio o a requerimiento de la misma, cuantos datos con trascendencia tributaria se desprendan de las actuaciones judiciales de las que conozcan, respetando, en su caso, el secreto de las diligencias sumariales.

4. El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo, así como la Secretaría de ambas comisiones, facilitarán a la Administración tributaria cuantos datos con trascendencia tributaria obtengan en el ejercicio de sus funciones, de oficio, con carácter general o mediante requerimiento individualizado en los términos que reglamentariamente se establezcan.

Los órganos de la Administración tributaria podrán utilizar la información suministrada para la regularización de la situación tributaria de los obligados en el curso del procedimiento de comprobación o de inspección, sin que sea necesario efectuar el requerimiento al que se refiere el apartado 3 del artículo anterior.

5. La cesión de datos de carácter personal que se deba efectuar a la Administración tributaria conforme a lo dispuesto en el artículo anterior, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito no será de aplicación lo dispuesto en el apartado 1 del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Artículo 95. *Carácter reservado de los datos con trascendencia tributaria.*

1. Los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de las sanciones que procedan, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto:

a) La colaboración con los órganos jurisdiccionales y el Ministerio Fiscal en la investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada.

b) La colaboración con otras Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias.

c) La colaboración con la Inspección de Trabajo y Seguridad Social y con las entidades gestoras y servicios comunes de la Seguridad Social en la lucha contra el fraude en la cotización y recaudación de las cuotas del sistema de Seguridad Social y contra el fraude en la obtención y disfrute de las prestaciones a cargo del sistema; así como para la determinación del nivel de aportación de cada usuario en las prestaciones del Sistema Nacional de Salud.

d) La colaboración con las Administraciones públicas para la prevención y lucha contra el delito fiscal y contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos o de la Unión Europea, incluyendo las medidas oportunas para prevenir, detectar y corregir el fraude, la corrupción y los conflictos de intereses que afecten a los intereses financieros de la Unión Europea.

e) La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido.

f) La protección de los derechos e intereses de los menores e incapacitados por los órganos jurisdiccionales o el Ministerio Fiscal.

g) La colaboración con el Tribunal de Cuentas en el ejercicio de sus funciones de fiscalización de la Agencia Estatal de Administración Tributaria.

h) La colaboración con los jueces y tribunales para la ejecución de resoluciones judiciales firmes. La solicitud judicial de información exigirá resolución expresa en la que, previa ponderación de los intereses públicos y privados afectados en el asunto de que se trate y por haberse agotado los demás medios o fuentes de conocimiento sobre la existencia de bienes y derechos del deudor, se motive la necesidad de recabar datos de la Administración tributaria.

i) La colaboración con el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, con la Comisión de Vigilancia de Actividades de Financiación del Terrorismo y con la Secretaría de ambas comisiones, en el ejercicio de sus funciones respectivas.

j) La colaboración con órganos o entidades de derecho público encargados de la recaudación de recursos públicos no tributarios para la correcta identificación de los

obligados al pago y con la Dirección General de Tráfico para la práctica de las notificaciones a los mismos, dirigidas al cobro de tales recursos.

k) La colaboración con las Administraciones públicas para el desarrollo de sus funciones, previa autorización de los obligados tributarios a que se refieran los datos suministrados.

l) La colaboración con la Intervención General de la Administración del Estado en el ejercicio de sus funciones de control de la gestión económico-financiera, el seguimiento del déficit público, el control de subvenciones y ayudas públicas y la lucha contra la morosidad en las operaciones comerciales de las entidades del Sector Público.

m) La colaboración con la Oficina de Recuperación y Gestión de Activos mediante la cesión de los datos, informes o antecedentes necesarios para la localización de los bienes y derechos susceptibles de ser embargados o decomisados en un determinado proceso penal, previa acreditación de esta circunstancia.

n) La colaboración con las entidades responsables de los procedimientos de adjudicación de contratos y concesión de subvenciones vinculadas a la ejecución del Plan de Recuperación, Transformación y Resiliencia, en relación con el análisis sistemático de riesgo de conflicto de interés.

2. En los casos de cesión previstos en el apartado anterior, la información de carácter tributario deberá ser suministrada preferentemente mediante la utilización de medios informáticos o telemáticos. Cuando las Administraciones públicas puedan disponer de la información por dichos medios, no podrán exigir a los interesados la aportación de certificados de la Administración tributaria en relación con dicha información.

3. La Administración tributaria adoptará las medidas necesarias para garantizar la confidencialidad de la información tributaria y su uso adecuado.

Cuantas autoridades o funcionarios tengan conocimiento de estos datos, informes o antecedentes estarán obligados al más estricto y completo sigilo respecto de ellos, salvo en los casos citados. Con independencia de las responsabilidades penales o civiles que pudieran derivarse, la infracción de este particular deber de sigilo se considerará siempre falta disciplinaria muy grave.

Cuando se aprecie la posible existencia de un delito no perseguible únicamente a instancia de persona agraviada, la Administración tributaria deducirá el tanto de culpa o remitirá al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito. También podrá iniciarse directamente el oportuno procedimiento mediante querella a través del Servicio Jurídico competente.

4. El carácter reservado de los datos establecido en este artículo no impedirá la publicidad de los mismos cuando ésta se derive de la normativa de la Unión Europea.

5. Los retenedores y obligados a realizar ingresos a cuenta sólo podrán utilizar los datos, informes o antecedentes relativos a otros obligados tributarios para el correcto cumplimiento y efectiva aplicación de la obligación de realizar pagos a cuenta. Dichos datos deberán ser comunicados a la Administración tributaria en los casos previstos en la normativa propia de cada tributo.

Salvo lo dispuesto en el párrafo anterior, los referidos datos, informes o antecedentes tienen carácter reservado. Los retenedores y obligados a realizar ingresos a cuenta quedan sujetos al más estricto y completo sigilo respecto de ellos.

6. La cesión de información en el ámbito de la asistencia mutua se regirá por lo dispuesto en el artículo 177 ter de esta Ley.

Artículo 95 bis. *Publicidad de situaciones de incumplimiento relevante de las obligaciones tributarias.*

1. La Administración Tributaria acordará la publicación periódica de listados comprensivos de deudores a la Hacienda Pública, incluidos los que tengan la condición de deudores al haber sido declarados responsables solidarios, por deudas o sanciones tributarias cuando concurran las siguientes circunstancias:

a) Que el importe total de las deudas y sanciones tributarias pendientes de ingreso, incluidas en su caso las que se hubieran exigido tras la declaración de responsabilidad solidaria, supere el importe de 600.000 euros.

b) Que dichas deudas o sanciones tributarias no hubiesen sido pagadas transcurrido el plazo original de ingreso en periodo voluntario.

En el supuesto de deudas incluidas en acuerdos de declaración de responsabilidad será necesario que haya transcurrido el plazo de pago del artículo 62.2 de esta Ley tras la notificación del acuerdo de declaración de responsabilidad y, en su caso, del acuerdo de exigencia de pago.

A efectos de lo dispuesto en este artículo no se incluirán aquellas deudas y sanciones tributarias que se encuentren aplazadas o suspendidas.

2. En dichos listados se incluirá la siguiente información:

a) La identificación de los deudores conforme al siguiente detalle:

– Personas Físicas: nombre apellidos y NIF.

– Personas Jurídicas y entidades del artículo 35.4 de esta Ley: razón o denominación social completa y NIF.

b) El importe conjunto de las deudas y sanciones pendientes de pago tenidas en cuenta a efectos de la publicación.

3. En el ámbito del Estado, la publicidad regulada en este artículo se referirá exclusivamente a los tributos de titularidad estatal para los que la aplicación de los tributos, el ejercicio de la potestad sancionadora y las facultades de revisión estén atribuidas en exclusiva a los órganos de la Administración Tributaria del Estado no habiendo existido delegación alguna de competencias en estos ámbitos a favor de las Comunidades Autónomas o Entes Locales.

La publicidad regulada en este artículo resultará de aplicación respecto a los tributos que integran la deuda aduanera.

4. La determinación de la concurrencia de los requisitos exigidos para la inclusión en el listado tomará como fecha de referencia el 31 de diciembre del año anterior al del acuerdo de publicación, cualquiera que sea la cantidad pendiente de ingreso a la fecha de dicho acuerdo.

La propuesta de inclusión en el listado será comunicada al deudor afectado, que podrá formular alegaciones en el plazo de 10 días contados a partir del siguiente al de recepción de la comunicación. A estos efectos será suficiente para entender realizada dicha comunicación la acreditación por parte de la Administración Tributaria de haber realizado un intento de notificación de la misma que contenga el texto íntegro de su contenido en el domicilio fiscal del interesado.

En el caso de que los deudores paguen la totalidad de la cantidad adeudada a la fecha de referencia antes de la finalización del plazo para formular alegaciones, no se incluirán en los listados comprensivos de deudores a la Hacienda Pública por deudas o sanciones tributarias.

Las alegaciones habrán de referirse exclusivamente a la existencia de errores materiales, de hecho o aritméticos en relación con los requisitos señalados en el apartado 1 o a los pagos efectuados por el deudor a que se refiere el párrafo anterior, debiéndose aportar en este caso justificación fehaciente de dichos pagos.

Como consecuencia del trámite de alegaciones, la Administración podrá acordar la rectificación del listado cuando se acredite fehacientemente que no concurren los requisitos legales determinados en el apartado 1 o cuando a la conclusión del plazo para formular alegaciones se hubiera satisfecho la totalidad de las deudas o sanciones tributarias.

Dicha rectificación también podrá ser acordada de oficio.

Practicadas las rectificaciones oportunas, se dictará el acuerdo de publicación.

La notificación del acuerdo se entenderá producida con su publicación y la del listado.

Mediante Orden Ministerial se establecerán la fecha de publicación, que deberá producirse en todo caso durante el primer semestre de cada año, y los correspondientes ficheros y registros.

La publicación se efectuará en todo caso por medios electrónicos, debiendo adoptarse las medidas necesarias para impedir la indexación de su contenido a través de motores de búsqueda en Internet y los listados dejarán de ser accesibles una vez transcurridos tres meses desde la fecha de publicación.

El tratamiento de datos necesarios para la publicación se sujetará a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como por su normativa de desarrollo.

5. En el ámbito de competencias del Estado, será competente para dictar los acuerdos de publicación regulados en este artículo el Director General de la Agencia Estatal de Administración Tributaria.

6. En la publicación del listado se especificará que la situación en el mismo reflejada es la existente a la fecha de referencia señalada en el apartado 4, sin que la publicación del listado resulte afectada por las actuaciones realizadas por el deudor con posterioridad a dicha fecha de referencia, salvo que se verifique el pago en los casos y con los requisitos señalados en dicho apartado.

Lo dispuesto en este artículo no afectará en modo alguno al régimen de impugnación establecido en esta Ley en relación con las actuaciones y procedimientos de los que se deriven las deudas y sanciones tributarias ni tampoco a las actuaciones y procedimientos de aplicación de los tributos iniciados o que se pudieran iniciar con posterioridad en relación con las mismas.

Las actuaciones desarrolladas en el procedimiento establecido en este artículo en orden a la publicación de la información en el mismo regulada no constituyen causa de interrupción a los efectos previstos en el artículo 68 de esta Ley.

7. El acuerdo de publicación del listado pondrá fin a la vía administrativa.

[. . .]

§ 65

Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 264, de 4 de noviembre de 2003
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2003-20254

[. . .]

TÍTULO V

Gestión patrimonial

[. . .]

CAPÍTULO V

Enajenación y gravamen

[. . .]

Sección 2.ª Enajenación de inmuebles

[. . .]

Artículo 138. *Procedimiento de enajenación.*

1. El expediente de enajenación de bienes inmuebles y derechos sobre los mismos pertenecientes al patrimonio de la Administración General del Estado será instruido por la Dirección General del Patrimonio del Estado que lo iniciará de oficio, por iniciativa propia o a solicitud de parte interesada en la adquisición, siempre que considere, justificándolo debidamente en el expediente, que el bien o derecho no es necesario para el uso general o el servicio público ni resulta conveniente su explotación. El acuerdo de incoación del procedimiento llevará implícita la declaración de alienabilidad de los bienes a que se refiera.

Podrá acordarse la enajenación de los inmuebles por lotes y, en los supuestos de enajenación directa, admitirse la entrega de otros inmuebles o derechos sobre los mismos en pago de parte del precio de venta, valorados de conformidad con el artículo 114 de esta ley.

2. El tipo de la subasta o el precio de la enajenación directa se fijarán por el órgano competente para la enajenación de acuerdo con la tasación aprobada. De igual forma, los pliegos que han de regir el concurso determinarán los criterios que hayan de tenerse en cuenta en la adjudicación, atendiendo a las directrices que resulten de las políticas públicas

de cuya aplicación se trate. En todo caso, los pliegos harán referencia a la situación física, jurídica y registral de la finca.

3. La convocatoria del procedimiento de enajenación se publicará gratuitamente en el "Boletín Oficial del Estado" y en el de la provincia en que radique el bien y se remitirá al ayuntamiento del correspondiente término municipal para su exhibición en el tablón de anuncios, sin perjuicio de la posibilidad de utilizar, además, otros medios de publicidad, atendida la naturaleza y características del bien.

La Dirección General del Patrimonio del Estado podrá establecer otros mecanismos complementarios tendentes a difundir información sobre los bienes inmuebles en proceso de venta, incluida la creación, con sujeción a las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, de ficheros con los datos de las personas que voluntaria y expresamente soliciten les sea remitida información sobre dichos bienes.

4. La suspensión del procedimiento, una vez efectuado el anuncio, sólo podrá efectuarse por Orden del Ministro de Hacienda, cuando se trate de bienes de la Administración General del Estado, o por acuerdo de los presidentes o directores de los organismos públicos, cuando se trate de bienes propios de éstos, con fundamento en documentos fehacientes o hechos acreditados que prueben la improcedencia de la venta.

5. El Ministro de Hacienda, a propuesta de la Dirección General del Patrimonio del Estado, o los presidentes o directores de los organismos públicos acordarán, previo informe de la Abogacía del Estado o del órgano al que corresponda el asesoramiento jurídico de las entidades públicas, la enajenación o su improcedencia, si considerasen perjudicial para el interés público la adjudicación en las condiciones propuestas o si, por razones sobrevenidas, considerasen necesario el bien para el cumplimiento de fines públicos, sin que la instrucción del expediente, la celebración de la subasta o la valoración de las proposiciones presentadas generen derecho alguno para quienes optaron a su compra.

[...]

§ 66

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Jefatura del Estado
«BOE» núm. 274, de 15 de noviembre de 2002
Última modificación: 1 de marzo de 2023
Referencia: BOE-A-2002-22188

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

La importancia que tienen los derechos de los pacientes como eje básico de las relaciones clínico-asistenciales se pone de manifiesto al constatar el interés que han demostrado por los mismos casi todas las organizaciones internacionales con competencia en la materia. Ya desde el fin de la Segunda Guerra Mundial, organizaciones como Naciones Unidas, UNESCO o la Organización Mundial de la Salud, o, más recientemente, la Unión Europea o el Consejo de Europa, entre muchas otras, han impulsado declaraciones o, en algún caso, han promulgado normas jurídicas sobre aspectos genéricos o específicos relacionados con esta cuestión. En este sentido, es necesario mencionar la trascendencia de la Declaración universal de derechos humanos, del año 1948, que ha sido el punto de referencia obligado para todos los textos constitucionales promulgados posteriormente o, en el ámbito más estrictamente sanitario, la Declaración sobre la promoción de los derechos de los pacientes en Europa, promovida el año 1994 por la Oficina Regional para Europa de la Organización Mundial de la Salud, aparte de múltiples declaraciones internacionales de mayor o menor alcance e influencia que se han referido a dichas cuestiones.

Últimamente, cabe subrayar la relevancia especial del Convenio del Consejo de Europa para la protección de los derechos humanos y la dignidad del ser humano respecto de las aplicaciones de la biología y la medicina (Convenio sobre los derechos del hombre y la biomedicina), suscrito el día 4 de abril de 1997, el cual ha entrado en vigor en el Reino de España el 1 de enero de 2000. Dicho Convenio es una iniciativa capital: en efecto, a diferencia de las distintas declaraciones internacionales que lo han precedido, es el primer instrumento internacional con carácter jurídico vinculante para los países que lo suscriben. Su especial valía reside en el hecho de que establece un marco común para la protección de los derechos humanos y la dignidad humana en la aplicación de la biología y la medicina. El

Convenio trata explícitamente, con detenimiento y extensión, sobre la necesidad de reconocer los derechos de los pacientes, entre los cuales resaltan el derecho a la información, el consentimiento informado y la intimidad de la información relativa a la salud de las personas, persiguiendo el alcance de una armonización de las legislaciones de los diversos países en estas materias; en este sentido, es absolutamente conveniente tener en cuenta el Convenio en el momento de abordar el reto de regular cuestiones tan importantes.

Es preciso decir, sin embargo, que la regulación del derecho a la protección de la salud, recogido por el artículo 43 de la Constitución de 1978, desde el punto de vista de las cuestiones más estrechamente vinculadas a la condición de sujetos de derechos de las personas usuarias de los servicios sanitarios, es decir, la plasmación de los derechos relativos a la información clínica y la autonomía individual de los pacientes en lo relativo a su salud, ha sido objeto de una regulación básica en el ámbito del Estado, a través de la Ley 14/1986, de 25 de abril, General de Sanidad.

De otra parte, esta Ley, a pesar de que fija básicamente su atención en el establecimiento y ordenación del sistema sanitario desde un punto de vista organizativo, dedica a esta cuestión diversas previsiones, entre las que destaca la voluntad de humanización de los servicios sanitarios. Así mantiene el máximo respeto a la dignidad de la persona y a la libertad individual, de un lado, y, del otro, declara que la organización sanitaria debe permitir garantizar la salud como derecho inalienable de la población mediante la estructura del Sistema Nacional de Salud, que debe asegurarse en condiciones de escrupuloso respeto a la intimidad personal y a la libertad individual del usuario, garantizando la confidencialidad de la información relacionada con los servicios sanitarios que se prestan y sin ningún tipo de discriminación.

A partir de dichas premisas, la presente Ley completa las previsiones que la Ley General de Sanidad enunció como principios generales. En este sentido, refuerza y da un trato especial al derecho a la autonomía del paciente. En particular, merece mención especial la regulación sobre instrucciones previas que contempla, de acuerdo con el criterio establecido en el Convenio de Oviedo, los deseos del paciente expresados con anterioridad dentro del ámbito del consentimiento informado. Asimismo, la Ley trata con profundidad todo lo referente a la documentación clínica generada en los centros asistenciales, subrayando especialmente la consideración y la concreción de los derechos de los usuarios en este aspecto.

En septiembre de 1997, en desarrollo de un convenio de colaboración entre el Consejo General del Poder Judicial y el Ministerio de Sanidad y Consumo, tuvo lugar un seminario conjunto sobre información y documentación clínica, en el que se debatieron los principales aspectos normativos y judiciales en la materia. Al mismo tiempo, se constituyó un grupo de expertos a quienes se encargó la elaboración de unas directrices para el desarrollo futuro de este tema. Este grupo suscribió un dictamen el 26 de noviembre de 1997, que ha sido tenido en cuenta en la elaboración de los principios fundamentales de esta Ley.

La atención que a estas materias otorgó en su día la Ley General de Sanidad supuso un notable avance como reflejan, entre otros, sus artículos 9, 10 y 61. Sin embargo, el derecho a la información, como derecho del ciudadano cuando demanda la atención sanitaria, ha sido objeto en los últimos años de diversas matizaciones y ampliaciones por Leyes y disposiciones de distinto tipo y rango, que ponen de manifiesto la necesidad de una reforma y actualización de la normativa contenida en la Ley General de Sanidad. Así, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, califica a los datos relativos a la salud de los ciudadanos como datos especialmente protegidos, estableciendo un régimen singularmente riguroso para su obtención, custodia y eventual cesión.

Esta defensa de la confidencialidad había sido ya defendida por la Directiva comunitaria 95/46, de 24 de octubre, en la que, además de reafirmarse la defensa de los derechos y libertades de los ciudadanos europeos, en especial de su intimidad relativa a la información relacionada con su salud, se apunta la presencia de otros intereses generales como los estudios epidemiológicos, las situaciones de riesgo grave para la salud de la colectividad, la investigación y los ensayos clínicos que, cuando estén incluidos en normas de rango de Ley, pueden justificar una excepción motivada a los derechos del paciente. Se manifiesta así una concepción comunitaria del derecho a la salud, en la que, junto al interés singular de cada

individuo, como destinatario por excelencia de la información relativa a la salud, aparecen también otros agentes y bienes jurídicos referidos a la salud pública, que deben ser considerados, con la relevancia necesaria, en una sociedad democrática avanzada. En esta línea, el Consejo de Europa, en su Recomendación de 13 de febrero de 1997, relativa a la protección de los datos médicos, después de afirmar que deben recogerse y procesarse con el consentimiento del afectado, indica que la información puede restringirse si así lo dispone una Ley y constituye una medida necesaria por razones de interés general.

Todas estas circunstancias aconsejan una adaptación de la Ley General de Sanidad con el objetivo de aclarar la situación jurídica y los derechos y obligaciones de los profesionales sanitarios, de los ciudadanos y de las instituciones sanitarias. Se trata de ofrecer en el terreno de la información y la documentación clínicas las mismas garantías a todos los ciudadanos del Estado, fortaleciendo con ello el derecho a la protección de la salud que reconoce la Constitución.

CAPÍTULO I

Principios generales

Artículo 1. *Ámbito de aplicación.*

La presente Ley tiene por objeto la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales, así como de los centros y servicios sanitarios, públicos y privados, en materia de autonomía del paciente y de información y documentación clínica.

Artículo 2. *Principios básicos.*

1. La dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica.

2. Toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes o usuarios. El consentimiento, que debe obtenerse después de que el paciente reciba una información adecuada, se hará por escrito en los supuestos previstos en la Ley.

3. El paciente o usuario tiene derecho a decidir libremente, después de recibir la información adecuada, entre las opciones clínicas disponibles.

4. Todo paciente o usuario tiene derecho a negarse al tratamiento, excepto en los casos determinados en la Ley. Su negativa al tratamiento constará por escrito.

5. Los pacientes o usuarios tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria.

6. Todo profesional que interviene en la actividad asistencial está obligado no sólo a la correcta prestación de sus técnicas, sino al cumplimiento de los deberes de información y de documentación clínica, y al respeto de las decisiones adoptadas libre y voluntariamente por el paciente.

7. La persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida.

Artículo 3. *Las definiciones legales.*

A efectos de esta Ley se entiende por:

Centro sanitario: el conjunto organizado de profesionales, instalaciones y medios técnicos que realiza actividades y presta servicios para cuidar la salud de los pacientes y usuarios.

Certificado médico: la declaración escrita de un médico que da fe del estado de salud de una persona en un determinado momento.

Consentimiento informado: la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud.

Documentación clínica: el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial.

Historia clínica: el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial.

Información clínica: todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla.

Informe de alta médica: el documento emitido por el médico responsable en un centro sanitario al finalizar cada proceso asistencial de un paciente, que especifica los datos de éste, un resumen de su historial clínico, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas.

Intervención en el ámbito de la sanidad: toda actuación realizada con fines preventivos, diagnósticos, terapéuticos, rehabilitadores o de investigación.

Libre elección: la facultad del paciente o usuario de optar, libre y voluntariamente, entre dos o más alternativas asistenciales, entre varios facultativos o entre centros asistenciales, en los términos y condiciones que establezcan los servicios de salud competentes, en cada caso.

Médico responsable: el profesional que tiene a su cargo coordinar la información y la asistencia sanitaria del paciente o del usuario, con el carácter de interlocutor principal del mismo en todo lo referente a su atención e información durante el proceso asistencial, sin perjuicio de las obligaciones de otros profesionales que participan en las actuaciones asistenciales.

Paciente: la persona que requiere asistencia sanitaria y está sometida a cuidados profesionales para el mantenimiento o recuperación de su salud.

Servicio sanitario: la unidad asistencial con organización propia, dotada de los recursos técnicos y del personal cualificado para llevar a cabo actividades sanitarias.

Usuario: la persona que utiliza los servicios sanitarios de educación y promoción de la salud, de prevención de enfermedades y de información sanitaria.

CAPÍTULO II

El derecho de información sanitaria

Artículo 4. *Derecho a la información asistencial.*

1. Los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la Ley. Además, toda persona tiene derecho a que se respete su voluntad de no ser informada. La información, que como regla general se proporcionará verbalmente dejando constancia en la historia clínica, comprende, como mínimo, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias.

2. La información clínica forma parte de todas las actuaciones asistenciales, será verdadera, se comunicará al paciente de forma comprensible y adecuada a sus necesidades y le ayudará a tomar decisiones de acuerdo con su propia y libre voluntad.

3. El médico responsable del paciente le garantiza el cumplimiento de su derecho a la información. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle.

Artículo 5. *Titular del derecho a la información asistencial.*

1. El titular del derecho a la información es el paciente. También serán informadas las personas vinculadas a él, por razones familiares o de hecho, en la medida que el paciente lo permita de manera expresa o tácita.

2. El paciente será informado, incluso en caso de incapacidad, de modo adecuado a sus posibilidades de comprensión, cumpliendo con el deber de informar también a su representante legal.

3. Cuando el paciente, según el criterio del médico que le asiste, carezca de capacidad para entender la información a causa de su estado físico o psíquico, la información se pondrá en conocimiento de las personas vinculadas a él por razones familiares o de hecho.

4. El derecho a la información sanitaria de los pacientes puede limitarse por la existencia acreditada de un estado de necesidad terapéutica. Se entenderá por necesidad terapéutica la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave.

Llegado este caso, el médico dejará constancia razonada de las circunstancias en la historia clínica y comunicará su decisión a las personas vinculadas al paciente por razones familiares o de hecho.

Artículo 6. *Derecho a la información epidemiológica.*

Los ciudadanos tienen derecho a conocer los problemas sanitarios de la colectividad cuando impliquen un riesgo para la salud pública o para su salud individual, y el derecho a que esta información se difunda en términos verdaderos, comprensibles y adecuados para la protección de la salud, de acuerdo con lo establecido por la Ley.

CAPÍTULO III

Derecho a la intimidad

Artículo 7. *El derecho a la intimidad.*

1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes.

CAPÍTULO IV

El respeto de la autonomía del paciente

Artículo 8. *Consentimiento informado.*

1. Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el artículo 4, haya valorado las opciones propias del caso.

2. El consentimiento será verbal por regla general.

Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente.

3. El consentimiento escrito del paciente será necesario para cada una de las actuaciones especificadas en el punto anterior de este artículo, dejando a salvo la posibilidad de incorporar anejos y otros datos de carácter general, y tendrá información suficiente sobre el procedimiento de aplicación y sobre sus riesgos.

4. Todo paciente o usuario tiene derecho a ser advertido sobre la posibilidad de utilizar los procedimientos de pronóstico, diagnóstico y terapéuticos que se le apliquen en un proyecto docente o de investigación, que en ningún caso podrá comportar riesgo adicional para su salud.

5. El paciente puede revocar libremente por escrito su consentimiento en cualquier momento.

Artículo 9. *Límites del consentimiento informado y consentimiento por representación.*

1. La renuncia del paciente a recibir información está limitada por el interés de la salud del propio paciente, de terceros, de la colectividad y por las exigencias terapéuticas del caso. Cuando el paciente manifieste expresamente su deseo de no ser informado, se respetará su voluntad haciendo constar su renuncia documentalmente, sin perjuicio de la obtención de su consentimiento previo para la intervención.

2. Los facultativos podrán llevar a cabo las intervenciones clínicas indispensables en favor de la salud del paciente, sin necesidad de contar con su consentimiento, en los siguientes casos:

a) Cuando existe riesgo para la salud pública a causa de razones sanitarias establecidas por la Ley. En todo caso, una vez adoptadas las medidas pertinentes, de conformidad con lo establecido en la Ley Orgánica 3/1986, se comunicarán a la autoridad judicial en el plazo máximo de 24 horas siempre que dispongan el internamiento obligatorio de personas.

b) Cuando existe riesgo inmediato grave para la integridad física o psíquica del enfermo y no es posible conseguir su autorización, consultando, cuando las circunstancias lo permitan, a sus familiares o a las personas vinculadas de hecho a él.

3. Se otorgará el consentimiento por representación en los siguientes supuestos:

a) Cuando el paciente no sea capaz de tomar decisiones, a criterio del médico responsable de la asistencia, o su estado físico o psíquico no le permita hacerse cargo de su situación. Si el paciente carece de representante legal, el consentimiento lo prestarán las personas vinculadas a él por razones familiares o de hecho.

b) Cuando el paciente tenga la capacidad modificada judicialmente y así conste en la sentencia.

c) Cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor, después de haber escuchado su opinión, conforme a lo dispuesto en el artículo 9 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

4. Cuando se trate de menores emancipados o mayores de 16 años que no se encuentren en los supuestos b) y c) del apartado anterior, no cabe prestar el consentimiento por representación.

No obstante lo dispuesto en el párrafo anterior, cuando se trate de una actuación de grave riesgo para la vida o salud del menor, según el criterio del facultativo, el consentimiento lo prestará el representante legal del menor, una vez oída y tenida en cuenta la opinión del mismo.

5. La práctica de ensayos clínicos y la práctica de técnicas de reproducción humana asistida se rigen por lo establecido con carácter general sobre la mayoría de edad y por las disposiciones especiales de aplicación.

6. En los casos en los que el consentimiento haya de otorgarlo el representante legal o las personas vinculadas por razones familiares o de hecho en cualquiera de los supuestos descritos en los apartados 3 a 5, la decisión deberá adoptarse atendiendo siempre al mayor beneficio para la vida o salud del paciente. Aquellas decisiones que sean contrarias a dichos intereses deberán ponerse en conocimiento de la autoridad judicial, directamente o a través del Ministerio Fiscal, para que adopte la resolución correspondiente, salvo que, por razones de urgencia, no fuera posible recabar la autorización judicial, en cuyo caso los profesionales sanitarios adoptarán las medidas necesarias en salvaguarda de la vida o salud del paciente, amparados por las causas de justificación de cumplimiento de un deber y de estado de necesidad.

7. La prestación del consentimiento por representación será adecuada a las circunstancias y proporcionada a las necesidades que haya que atender, siempre en favor del paciente y con respeto a su dignidad personal. El paciente participará en la medida de lo posible en la toma de decisiones a lo largo del proceso sanitario. Si el paciente es una persona con discapacidad, se le ofrecerán las medidas de apoyo pertinentes, incluida la información en formatos adecuados, siguiendo las reglas marcadas por el principio del

diseño para todos de manera que resulten accesibles y comprensibles a las personas con discapacidad, para favorecer que pueda prestar por sí su consentimiento.

Artículo 10. *Condiciones de la información y consentimiento por escrito.*

1. El facultativo proporcionará al paciente, antes de recabar su consentimiento escrito, la información básica siguiente:

a) Las consecuencias relevantes o de importancia que la intervención origina con seguridad.
b) Los riesgos relacionados con las circunstancias personales o profesionales del paciente.
c) Los riesgos probables en condiciones normales, conforme a la experiencia y al estado de la ciencia o directamente relacionados con el tipo de intervención.
d) Las contraindicaciones.

2. El médico responsable deberá ponderar en cada caso que cuanto más dudoso sea el resultado de una intervención más necesario resulta el previo consentimiento por escrito del paciente.

Artículo 11. *Instrucciones previas.*

1. Por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo. El otorgante del documento puede designar, además, un representante para que, llegado el caso, sirva como interlocutor suyo con el médico o el equipo sanitario para procurar el cumplimiento de las instrucciones previas.
2. Cada servicio de salud regulará el procedimiento adecuado para que, llegado el caso, se garantice el cumplimiento de las instrucciones previas de cada persona, que deberán constar siempre por escrito.
3. No serán aplicadas las instrucciones previas contrarias al ordenamiento jurídico, a la «lex artis», ni las que no se correspondan con el supuesto de hecho que el interesado haya previsto en el momento de manifestarlas. En la historia clínica del paciente quedará constancia razonada de las anotaciones relacionadas con estas previsiones.
4. Las instrucciones previas podrán revocarse libremente en cualquier momento dejando constancia por escrito.
5. Con el fin de asegurar la eficacia en todo el territorio nacional de las instrucciones previas manifestadas por los pacientes y formalizadas de acuerdo con lo dispuesto en la legislación de las respectivas Comunidades Autónomas, se creará en el Ministerio de Sanidad y Consumo el Registro nacional de instrucciones previas que se regirá por las normas que reglamentariamente se determinen, previo acuerdo del Consejo Interterritorial del Sistema Nacional de Salud.

Artículo 12. *Información en el Sistema Nacional de Salud.*

1. Además de los derechos reconocidos en los artículos anteriores, los pacientes y los usuarios del Sistema Nacional de Salud tendrán derecho a recibir información sobre los servicios y unidades asistenciales disponibles, su calidad y los requisitos de acceso a ellos.
2. Los servicios de salud dispondrán en los centros y servicios sanitarios de una guía o carta de los servicios en la que se especifiquen los derechos y obligaciones de los usuarios, las prestaciones disponibles, las características asistenciales del centro o del servicio, y sus dotaciones de personal, instalaciones y medios técnicos.
Se facilitará a todos los usuarios información sobre las guías de participación y sobre sugerencias y reclamaciones.
3. Cada servicio de salud regulará los procedimientos y los sistemas para garantizar el efectivo cumplimiento de las previsiones de este artículo.

Artículo 13. *Derecho a la información para la elección de médico y de centro.*

Los usuarios y pacientes del Sistema Nacional de Salud, tanto en la atención primaria como en la especializada, tendrán derecho a la información previa correspondiente para elegir médico, e igualmente centro, con arreglo a los términos y condiciones que establezcan los servicios de salud competentes.

CAPÍTULO V

La historia clínica

Artículo 14. *Definición y archivo de la historia clínica.*

1. La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.

2. Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.

3. Las Administraciones sanitarias establecerán los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura.

4. Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental.

Artículo 15. *Contenido de la historia clínica de cada paciente.*

1. La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada.

2. La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud.

El contenido mínimo de la historia clínica será el siguiente:

a) La documentación relativa a la hoja clínicoestadística.
b) La autorización de ingreso.
c) El informe de urgencia.
d) La anamnesis y la exploración física.
e) La evolución.
f) Las órdenes médicas.
g) La hoja de interconsulta.
h) Los informes de exploraciones complementarias.
i) El consentimiento informado.
j) El informe de anestesia.
k) El informe de quirófano o de registro del parto.
l) El informe de anatomía patológica.
m) La evolución y planificación de cuidados de enfermería.
n) La aplicación terapéutica de enfermería.
ñ) El gráfico de constantes.
o) El informe clínico de alta.

Los párrafos b), c), i), j), k), l), ñ) y o) sólo serán exigibles en la cumplimentación de la historia clínica cuando se trate de procesos de hospitalización o así se disponga.

3. Cuando se trate del nacimiento, la historia clínica incorporará, además de la información a la que hace referencia este apartado, los resultados de las pruebas biométricas, médicas o analíticas que resulten, en su caso, necesarias para determinar el vínculo de filiación con la madre, en los términos que se establezcan reglamentariamente.

4. La historia clínica se llevará con criterios de unidad y de integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial.

5. Cuando la atención sanitaria prestada lo sea a consecuencia de violencia ejercida contra personas menores de edad, la historia clínica especificará esta circunstancia, además de la información a la que hace referencia este apartado.

Artículo 16. *Usos de la historia clínica.*

1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso.

Artículo 17. *La conservación de la documentación clínica.*

1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el

tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

No obstante, los datos de la historia clínica relacionados con el nacimiento del paciente, incluidos los resultados de las pruebas biométricas, médicas o analíticas que en su caso resulten necesarias para determinar el vínculo de filiación con la madre, no se destruirán, trasladándose una vez conocido el fallecimiento del paciente, a los archivos definitivos de la Administración correspondiente, donde se conservarán con las debidas medidas de seguridad a los efectos de la legislación de protección de datos.

2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas.

Sin perjuicio del derecho al que se refiere el artículo siguiente, los datos de la historia clínica relacionados con las pruebas biométricas, médicas o analíticas que resulten necesarias para determinar el vínculo de filiación con la madre del recién nacido, sólo podrán ser comunicados a petición judicial, dentro del correspondiente proceso penal o en caso de reclamación o impugnación judicial de la filiación materna.

3. Los profesionales sanitarios tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes.

4. La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario.

5. Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen.

6. Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

Artículo 18. *Derechos de acceso a la historia clínica.*

1. El paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos.

2. El derecho de acceso del paciente a la historia clínica puede ejercerse también por representación debidamente acreditada.

3. El derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

4. Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.

Artículo 19. *Derechos relacionados con la custodia de la historia clínica.*

El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la

integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley.

CAPÍTULO VI

Informe de alta y otra documentación clínica

Artículo 20. *Informe de alta.*

Todo paciente, familiar o persona vinculada a él, en su caso, tendrá el derecho a recibir del centro o servicio sanitario, una vez finalizado el proceso asistencial, un informe de alta con los contenidos mínimos que determina el artículo 3. Las características, requisitos y condiciones de los informes de alta se determinarán reglamentariamente por las Administraciones sanitarias autonómicas.

Artículo 21. *El alta del paciente.*

1. En caso de no aceptar el tratamiento prescrito, se propondrá al paciente o usuario la firma del alta voluntaria. Si no la firmara, la dirección del centro sanitario, a propuesta del médico responsable, podrá disponer el alta forzosa en las condiciones reguladas por la Ley.

El hecho de no aceptar el tratamiento prescrito no dará lugar al alta forzosa cuando existan tratamientos alternativos, aunque tengan carácter paliativo, siempre que los preste el centro sanitario y el paciente acepte recibirlos. Estas circunstancias quedarán debidamente documentadas.

2. En el caso de que el paciente no acepte el alta, la dirección del centro, previa comprobación del informe clínico correspondiente, oirá al paciente y, si persiste en su negativa, lo pondrá en conocimiento del juez para que confirme o revoque la decisión.

Artículo 22. *Emisión de certificados médicos.*

Todo paciente o usuario tiene derecho a que se le faciliten los certificados acreditativos de su estado de salud. Éstos serán gratuitos cuando así lo establezca una disposición legal o reglamentaria.

Artículo 23. *Obligaciones profesionales de información técnica, estadística y administrativa.*

Los profesionales sanitarios, además de las obligaciones señaladas en materia de información clínica, tienen el deber de cumplimentar los protocolos, registros, informes, estadísticas y demás documentación asistencial o administrativa, que guarden relación con los procesos clínicos en los que intervienen, y los que requieran los centros o servicios de salud competentes y las autoridades sanitarias, comprendidos los relacionados con la investigación médica y la información epidemiológica.

Disposición adicional primera. *Carácter de legislación básica.*

Esta Ley tiene la condición de básica, de conformidad con lo establecido en el artículo 149.1.1.ª y 16.ª de la Constitución.

El Estado y las Comunidades Autónomas adoptarán, en el ámbito de sus respectivas competencias, las medidas necesarias para la efectividad de esta Ley.

Disposición adicional segunda. *Aplicación supletoria.*

Las normas de esta Ley relativas a la información asistencial, la información para el ejercicio de la libertad de elección de médico y de centro, el consentimiento informado del paciente y la documentación clínica, serán de aplicación supletoria en los proyectos de investigación médica, en los procesos de extracción y trasplante de órganos, en los de aplicación de técnicas de reproducción humana asistida y en los que carezcan de regulación especial.

Disposición adicional tercera. *Coordinación de las historias clínicas.*

El Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición.

Disposición adicional cuarta. *Necesidades asociadas a la discapacidad.*

El Estado y las Comunidades Autónomas, dentro del ámbito de sus respectivas competencias, dictarán las disposiciones precisas para garantizar a los pacientes o usuarios con necesidades especiales, asociadas a la discapacidad, los derechos en materia de autonomía, información y documentación clínica regulados en esta Ley.

Disposición adicional quinta. *Información y documentación sobre medicamentos y productos sanitarios.*

La información, la documentación y la publicidad relativas a los medicamentos y productos sanitarios, así como el régimen de las recetas y de las órdenes de prescripción correspondientes, se regularán por su normativa específica, sin perjuicio de la aplicación de las reglas establecidas en esta Ley en cuanto a la prescripción y uso de medicamentos o productos sanitarios durante los procesos asistenciales.

Disposición adicional sexta. *Régimen sancionador.*

Las infracciones de lo dispuesto por la presente Ley quedan sometidas al régimen sancionador previsto en el capítulo VI del Título I de la Ley 14/1986, General de Sanidad, sin perjuicio de la responsabilidad civil o penal y de la responsabilidad profesional o estatutaria procedentes en derecho.

Disposición transitoria única. *Informe de alta.*

El informe de alta se regirá por lo dispuesto en la Orden del Ministerio de Sanidad, de 6 de septiembre de 1984, mientras no se desarrolle legalmente lo dispuesto en el artículo 20 de esta Ley.

Disposición derogatoria única. *Derogación general y de preceptos concretos.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en la presente Ley y, concretamente, los apartados 5, 6, 8, 9 y 11 del artículo 10, el apartado 4 del artículo 11 y el artículo 61 de la Ley 14/1986, General de Sanidad.

Disposición final única. *Entrada en vigor.*

La presente Ley entrará en vigor en el plazo de seis meses a partir del día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 67

Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 73, de 26 de marzo de 2002
Última modificación: 23 de septiembre de 2011
Referencia: BOE-A-2002-5852

[. . .]

CAPÍTULO III

Funcionamiento de las asociaciones

[. . .]

Artículo 14. *Obligaciones documentales y contables.*

1. Las asociaciones han de disponer de una relación actualizada de sus asociados, llevar una contabilidad que permita obtener la imagen fiel del patrimonio, del resultado y de la situación financiera de la entidad, así como las actividades realizadas, efectuar un inventario de sus bienes y recoger en un libro las actas de las reuniones de sus órganos de gobierno y representación. Deberán llevar su contabilidad conforme a las normas específicas que les resulten de aplicación.

2. Los asociados podrán acceder a toda la documentación- que se relaciona en el apartado anterior, a través de los órganos de representación, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

3. Las cuentas de la asociación se aprobarán anualmente por la Asamblea General.

[. . .]

CAPÍTULO V

Registros de Asociaciones

[. . .]

Artículo 29. *Publicidad.*

1. Los Registros de Asociaciones son públicos.

2. La publicidad se hará efectiva mediante certificación del contenido de los asientos, por nota simple informativa o por copia de los asientos y de los documentos depositados en los

Registros o por medios informáticos o telemáticos que se ajustará a los requisitos establecidos en la normativa vigente en materia de protección de datos de carácter personal.

[. . .]

§ 68

Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 11, de 13 de enero de 2000
Última modificación: 3 de enero de 2025
Referencia: BOE-A-2000-641

[. . .]

TÍTULO VII

De la ejecución de las medidas

[. . .]

CAPÍTULO II

Reglas para la ejecución de las medidas

[. . .]

Artículo 48. *Expediente personal de la persona sometida a la ejecución de una medida.*

1. La entidad pública abrirá un expediente personal único a cada menor respecto del cual tenga encomendada la ejecución de una medida, en el que se recogerán los informes relativos a aquél, las resoluciones judiciales que le afecten y el resto de la documentación generada durante la ejecución.

2. Dicho expediente tendrá carácter reservado y solamente tendrán acceso al mismo el Defensor del Pueblo o institución análoga de la correspondiente Comunidad Autónoma, los Jueces de Menores competentes, el Ministerio Fiscal y las personas que intervengan en la ejecución y estén autorizadas por la entidad pública de acuerdo con sus normas de organización. El menor, su letrado y, en su caso, su representante legal, también tendrán acceso al expediente.

3. La recogida, cesión y tratamiento automatizado de datos de carácter personal de las personas a las que se aplique la presente Ley, sólo podrá realizarse en ficheros informáticos de titularidad pública dependientes de las entidades públicas de protección de menores, Administraciones y Juzgados de Menores competentes o del Ministerio Fiscal, y se regirá por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Cáracter Personal, y sus normas de desarrollo.

[. . .]

Disposición adicional tercera. *Creación del Registro Central de Menores.*

En el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes se llevará un Registro Central de sentencias, medidas cautelares, requisitorias y rebeldías dictadas o acordadas en todos los procesos tramitados con arreglo a la presente ley orgánica. El acceso a los datos de este Registro se ajustará a lo establecido en la normativa que regule el Sistema de registros administrativos de apoyo a la Administración de Justicia y el Registro Central de Delincuentes Sexuales y de Trata de Seres Humanos, y en la legislación aplicable en materia de protección de datos personales.

Téngase en cuenta que el Registro Central de Menores previsto en esta disposición, entrará en funcionamiento el 8 de noviembre de 2025, según establece la disposición transitoria única de la Ley Orgánica 4/2024, de 18 de octubre. Ref. BOE-A-2024-21414

[. . .]

§ 69

Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 10, de 12 de enero de 2000
Última modificación: 19 de marzo de 2025
Referencia: BOE-A-2000-544

[. . .]

TÍTULO II

Régimen jurídico de los extranjeros

CAPÍTULO I

De la entrada y salida del territorio español

Artículo 25. *Requisitos para la entrada en territorio español.*

1. El extranjero que pretenda entrar en España deberá hacerlo por los puestos habilitados al efecto, hallarse provisto del pasaporte o documento de viaje que acredite su identidad, que se considere válido para tal fin en virtud de convenios internacionales suscritos por España y no estar sujeto a prohibiciones expresas. Asimismo, deberá presentar los documentos que se determinen reglamentariamente que justifiquen el objeto y condiciones de estancia, y acreditar medios de vida suficientes para el tiempo que pretenda permanecer en España, o estar en condiciones de obtener legalmente dichos medios.

2. Salvo en los casos en que se establezca lo contrario en los convenios internacionales suscritos por España o en la normativa de la Unión Europea, será preciso, además, un visado.

No será exigible el visado cuando el extranjero se encuentre provisto de la tarjeta de identidad de extranjero o, excepcionalmente, de una autorización de regreso.

3. Lo dispuesto en los párrafos anteriores no será de aplicación a los extranjeros que soliciten acogerse al derecho de asilo en el momento de su entrada en España, cuya concesión se regirá por lo dispuesto en su normativa específica.

4. Se podrá autorizar la entrada en España de los extranjeros que no reúnan los requisitos establecidos en los párrafos anteriores cuando existan razones excepcionales de índole humanitaria, interés público o cum plimiento de compromisos adquiridos por España. En estos casos, se procederá a hacer entrega al extranjero de la documentación que se establezca reglamentariamente.

5. La entrada en territorio nacional de los extranjeros a los que no les sea de aplicación el régimen comunitario, podrá ser registrada por las autoridades españolas a los efectos de

control de su período de permanencia legal en España, de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[. . .]

Artículo 28. *De la salida de España.*

1. Las salidas del territorio español podrán realizarse libremente, excepto en los casos previstos en el Código Penal y en la presente Ley. La salida de los extranjeros a los que no les sea de aplicación el régimen comunitario, podrá ser registrada por las autoridades españolas a los efectos de control de su período de permanencia legal en España de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Excepcionalmente, el Ministro del Interior podrá prohibir la salida del territorio español por razones de seguridad nacional o de salud pública. La instrucción y resolución de los expedientes de prohibición tendrá siempre carácter individual.

3. La salida será obligatoria en los siguientes supuestos:

a) Expulsión del territorio español por orden judicial, en los casos previstos en el Código Penal.

b) Expulsión o devolución acordadas por resolución administrativa en los casos previstos en la presente Ley.

c) Denegación administrativa de las solicitudes formuladas por el extranjero para continuar permaneciendo en territorio español, o falta de autorización para encontrarse en España.

d) Cumplimiento del plazo en el que un trabajador extranjero se hubiera comprometido a regresar a su país de origen en el marco de un programa de retorno voluntario.

[. . .]

Disposición adicional quinta. *Acceso a la información, colaboración entre Administraciones públicas y gestión informática de los procedimientos.*

1. En el cumplimiento de los fines que tienen encomendadas, y con pleno respeto a la legalidad vigente, las Administraciones públicas, dentro de su ámbito competencial, colaborarán en la cesión de datos relativos a las personas que sean consideradas interesados en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo.

2. Para la exclusiva finalidad de cumplimentar las actuaciones que los órganos de la Administración General del Estado competentes en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo tienen encomendadas, la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social y el Instituto Nacional de Estadística, este último en lo relativo al Padrón Municipal de Habitantes, facilitarán a aquéllos el acceso directo a los ficheros en los que obren datos que hayan de constar en dichos expedientes, y sin que sea preciso el consentimiento de los interesados, de acuerdo con la legislación sobre protección de datos.

Igualmente, los anteriores organismos facilitarán a las Comunidades Autónomas la información necesaria para ejercer sus competencias sobre autorizaciones iniciales de trabajo sin que tampoco sea preciso el consentimiento de los interesados.

3. La tramitación de los procedimientos en materia de extranjería derivados del cumplimiento de lo dispuesto en la presente Ley Orgánica, se realizará sobre una aplicación informática común cuya implantación y coordinación respecto de los restantes Departamentos implicados corresponderá al Ministerio de Trabajo e Inmigración. Dicha aplicación, garantizando la protección de datos de carácter personal, registrará la información y datos relativos a los extranjeros y ciudadanos de la Unión Europea residentes en España y sus autorizaciones, impulsará el cumplimiento de lo establecido por la legislación en materia de acceso electrónico de los ciudadanos a los servicios públicos y permitirá el conocimiento, en tiempo real, de la situación de las solicitudes de autorización

reguladas en esta Ley por parte de los órganos administrativos que sean competentes en cada una de las fases del mismo, así como su intervención en la fase que recaiga dentro de su ámbito de competencias. Asimismo, la aplicación informática permitirá la generación de bases de datos estadísticas por las administraciones intervinientes para la obtención de la información actualizada y fiable sobre las magnitudes relativas a la inmigración y la extranjería.

En cumplimiento de lo establecido por la normativa comunitaria sobre la materia, la tramitación de procedimientos relativos a visados de tránsito y de estancia se realizará sobre la aplicación informática específicamente creada a los efectos, dependiente del Ministerio de Asuntos Exteriores y de Cooperación, que estará interconectada con la aplicación informática común, en orden a que en la base de datos de esta última conste información sobre los datos de los visados solicitados y concedidos en las Oficinas consulares o Misiones diplomáticas españolas en el exterior.

El Ministerio del Interior, de acuerdo con sus competencias en materia de orden público, seguridad pública y seguridad nacional, mantendrá un Registro central de extranjeros. Reglamentariamente, se establecerá la interconexión que, en su caso, resulte necesaria para que en la aplicación informática común conste la información que pueda repercutir en la situación administrativa de los extranjeros en España.

4. Cuando las Comunidades Autónomas, en el ámbito de sus competencias, intervengan en alguno de los procedimientos regulados en esta Ley, se garantizará que su participación en los procedimientos informatizados responda a estándares comunes que garanticen la necesaria coordinación de la actuación de todos los órganos administrativos intervinientes. Igualmente, la aplicación informática común dará acceso a las Comunidades Autónomas con competencias en materia de autorización de trabajo a la información necesaria para el ejercicio de sus competencias, entre la que se encontrará aquella relativa a la concesión y extinción de autorizaciones de reagrupación familiar concedidas en su territorio así como de las altas en Seguridad Social de las autorizaciones de trabajo iniciales concedidas por ellas.

5. El Observatorio Permanente de la Inmigración aunará el conjunto de la información estadística disponible en materia de extranjería, inmigración, protección internacional y nacionalidad, con independencia de la Administración Pública, Departamento ministerial u Organismo responsable de su elaboración, con la finalidad de servir como sistema de análisis e intercambio de la información cualitativa y cuantitativa relacionada con los movimientos migratorios al servicio de las entidades responsables de gestionar las políticas públicas en dichas materias.

[. . .]

§ 70

Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 167, de 14 de julio de 1998
Última modificación: 3 de enero de 2025
Referencia: BOE-A-1998-16718

Téngase en cuenta que, a partir del 1 de octubre de 2015, todas las referencias a Secretarios judiciales deberán entenderse hechas a Letrados de la Administración de Justicia, según establece la disposición adicional primera de la Ley Orgánica 7/2015, de 21 de julio. Ref. BOE-A-2015-8167

TÍTULO I

Del orden jurisdiccional contencioso-administrativo

[. . .]

CAPÍTULO II

Órganos y competencias

[. . .]

Artículo 10. *Competencias de las Salas de lo Contencioso-Administrativo de los Tribunales Superiores de Justicia.*

1. Las Salas de lo Contencioso-Administrativo de los Tribunales Superiores de Justicia conocerán en única instancia de los recursos que se deduzcan en relación con:

a) Los actos de las Entidades locales y de las Administraciones de las Comunidades Autónomas, cuyo conocimiento no esté atribuido a los Juzgados de lo Contencioso-Administrativo.

b) Las disposiciones generales emanadas de las Comunidades Autónomas y de las Entidades locales.

c) Los actos y disposiciones de los órganos de gobierno de las asambleas legislativas de las Comunidades Autónomas, y de las instituciones autonómicas análogas al Tribunal de Cuentas y al Defensor del Pueblo, en materia de personal, administración y gestión patrimonial.

d) Los actos y resoluciones dictados por los Tribunales Económico-Administrativos Regionales y Locales que pongan fin a la vía económico-administrativa.

e) Las resoluciones dictadas por el Tribunal Económico-Administrativo Central en materia de tributos cedidos.

f) Los actos y disposiciones de las Juntas Electorales Provinciales y de Comunidades Autónomas, así como los recursos contencioso-electorales contra acuerdos de las Juntas Electorales sobre proclamación de electos y elección y proclamación de Presidentes de Corporaciones locales, en los términos de la legislación electoral.

g) Los convenios entre Administraciones públicas cuyas competencias se ejerzan en el ámbito territorial de la correspondiente Comunidad Autónoma.

h) La prohibición o la propuesta de modificación de reuniones previstas en la Ley Orgánica 9/1983, de 15 de julio, Reguladora del Derecho de Reunión.

i) Los actos y resoluciones dictados por órganos de la Administración General del Estado cuya competencia se extienda a todo el territorio nacional y cuyo nivel orgánico sea inferior al de Ministro o Secretario de Estado en materias de personal, propiedades especiales y expropiación forzosa.

j) Los actos y resoluciones de los órganos de las Comunidades Autónomas competentes para la aplicación de la Ley de Defensa de la Competencia.

k) Las resoluciones dictadas por el órgano competente para la resolución de recursos en materia de contratación previsto en el artículo 311 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, en relación con los contratos incluidos en el ámbito competencial de las Comunidades Autónomas o de las Corporaciones locales.

l) Las resoluciones dictadas por los Tribunales Administrativos Territoriales de Recursos Contractuales.

m) Los actos y disposiciones dictados por las autoridades independientes autonómicas u órganos competentes de las comunidades autónomas referidos en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

n) Cualesquiera otras actuaciones administrativas no atribuidas expresamente a la competencia de otros órganos de este orden jurisdiccional.

2. Conocerán, en segunda instancia, de las apelaciones promovidas contra sentencias y autos dictados por los Juzgados de lo Contencioso-administrativo, y de los correspondientes recursos de queja.

3. También les corresponde, con arreglo a lo establecido en esta Ley, el conocimiento de los recursos de revisión contra las sentencias firmes de los Juzgados de lo Contencioso-administrativo.

4. Conocerán de las cuestiones de competencia entre los Juzgados de lo Contencioso-administrativo con sede en la Comunidad Autónoma.

5. Conocerán del recurso de casación para la unificación de doctrina previsto en el artículo 99.

6. Conocerán del recurso de casación en interés de la ley previsto en el artículo 101.

7. Conocerán de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.

8. **(Anulado)**

Artículo 11.

1. La Sala de lo Contencioso-administrativo de la Audiencia Nacional conocerá en única instancia:

a) De los recursos que se deduzcan en relación con las disposiciones generales y los actos de los Ministros, aun cuando se adopten previo informe o acuerdo del Consejo de Ministros o de las Comisiones Delegadas del Gobierno, y de los Secretarios de Estado, en general y en materia de personal cuando se refieran al nacimiento o extinción de la relación de servicio de funcionarios de carrera. Asimismo, conocerá de los recursos contra los actos de cualesquiera órganos centrales del Ministerio de Defensa referidos a ascensos, orden y antigüedad en el escalafón y destinos.

Téngase en cuenta que esta última actualización de la letra a) del apartado 1, establecida por el art. 21.1 de la Ley Orgánica 1/2025, de 2 de enero. Ref. BOE-A-2025-76, entra en vigor el 3 de abril de 2025, según determina su disposición final 38.1

Redacción anterior:

"a) De los recursos que se deduzcan en relación con las disposiciones generales y los actos de los Ministros y de los Secretarios de Estado en general y en materia de personal cuando se refieran al nacimiento o extinción de la relación de servicio de funcionarios de carrera. Asimismo conocerá de los recursos contra los actos de cualesquiera órganos centrales del Ministerio de Defensa referidos a ascensos, orden y antigüedad en el escalafonamiento y destinos."

b) De los recursos contra los actos de los Ministros y Secretarios de Estado cuando rectifiquen en vía de recurso o en procedimiento de fiscalización o de tutela los dictados por órganos o entes distintos con competencia en todo el territorio nacional.

c) De los recursos en relación con los convenios entre Administraciones públicas no atribuidos a los Tribunales Superiores de Justicia.

d) De los actos de naturaleza económico-administrativa dictados por el Ministro de Economía y Hacienda y por el Tribunal Económico-Administrativo Central, con excepción de lo dispuesto en el artículo 10.1.e).

e) De los recursos contra los actos dictados por la Comisión de Vigilancia de Actividades de Financiación del Terrorismo, y de la autorización de prórroga de los plazos de las medidas de dicha Comisión, conforme a lo previsto en la Ley de Prevención y Bloqueo de la Financiación del Terrorismo.

f) Las resoluciones dictadas por el Tribunal Administrativo Central de Recursos Contractuales, con excepción de lo dispuesto en el artículo 10.1.k).

g) De los recursos contra los actos del Banco de España, de la Comisión Nacional del Mercado de Valores y del FROB adoptados conforme a lo previsto en la Ley 11/2015, de 18 de junio, de recuperación y resolución de entidades de crédito y empresas de servicios de inversión.

h) De los recursos interpuestos por la Comisión Nacional de los Mercados y de la Competencia en defensa de la unidad de mercado.

i) **(Anulado)**

2. Conocerá, en segunda instancia, de las apelaciones contra autos y sentencias dictados por los Juzgados Centrales de lo Contencioso-administrativo y de los correspondientes recursos de queja.

3. Conocerá de los recursos de revisión contra sentencias firmes dictadas por los Juzgados Centrales de lo Contencioso-administrativo.

4. También conocerá de las cuestiones de competencia que se puedan plantear entre los Juzgados Centrales de lo Contencioso-administrativo.

5. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la Agencia Española de Protección de Datos.

Artículo 12.

1. La Sala de lo Contencioso-administrativo del Tribunal Supremo conocerá en única instancia de los recursos que se deduzcan en relación con:

a) Los actos y disposiciones del Consejo de Ministros y de las Comisiones Delegadas del Gobierno.

b) Los actos y disposiciones del Consejo General del Poder Judicial y del Fiscal General del Estado.

c) Los actos y disposiciones en materia de personal, administración y gestión patrimonial adoptados por los órganos competentes del Congreso de los Diputados, del Senado, del Tribunal Constitucional, del Tribunal de Cuentas y del Defensor del Pueblo.

2. Conocerá también de:

a) Los recursos de casación de cualquier modalidad, en los términos establecidos por esta Ley, y los correspondientes recursos de queja.

b) Los recursos de casación y revisión contra las resoluciones dictadas por el Tribunal de Cuentas, con arreglo a lo establecido en su Ley de Funcionamiento.

c) Los recursos de revisión contra sentencias firmes dictadas por las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia, de la Audiencia Nacional y del Tribunal Supremo, salvo lo dispuesto en el artículo 61.1.1º de la Ley Orgánica del Poder Judicial.

3. Asimismo conocerá de:

a) Los recursos que se deduzcan en relación con los actos y disposiciones de la Junta Electoral Central, así como los recursos contencioso-electorales que se deduzcan contra los acuerdos sobre proclamación de electos en los términos previstos en la legislación electoral.

b) Los recursos deducidos contra actos de las Juntas Electorales adoptados en el procedimiento para elección de miembros de las Salas de Gobierno de los Tribunales, en los términos de la Ley Orgánica del Poder Judicial.

4. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por el Consejo General del Poder Judicial.

[. . .]

TÍTULO V

Procedimientos especiales

CAPÍTULO I

Procedimiento para la protección de los derechos fundamentales de la persona

[. . .]

Artículo 122 ter. *Procedimiento de autorización judicial de conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos.*

1. El procedimiento para obtener la autorización judicial a que se refiere la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, se iniciará con la solicitud de la autoridad de protección de datos dirigida al Tribunal competente para que se pronuncie acerca de la conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos con el Derecho de la Unión Europea. La solicitud irá acompañada de copia del expediente que se encontrase pendiente de resolución ante la autoridad de protección de datos.

2. Serán partes en el procedimiento, además de la autoridad de protección de datos, quienes lo fueran en el procedimiento tramitado ante ella y, en todo caso, la Comisión Europea.

3. El acuerdo de admisión o inadmisión a trámite del procedimiento confirmará, modificará o levantará la suspensión del procedimiento por posible vulneración de la normativa de protección de datos tramitado ante la autoridad de protección de datos, del que trae causa este procedimiento de autorización judicial.

4. Admitida a trámite la solicitud, el Tribunal competente lo notificará a la autoridad de protección de datos a fin de que dé traslado a quienes interviniesen en el procedimiento tramitado ante la misma para que se personen en el plazo de tres días. Igualmente, se dará traslado a la Comisión Europea a los mismos efectos.

5. Concluido el plazo mencionado en la letra anterior, se dará traslado de la solicitud de autorización a las partes personadas a fin de que en el plazo de diez días aleguen lo que estimen procedente, pudiendo solicitar en ese momento la práctica de las pruebas que estimen necesarias.

6. Transcurrido el período de prueba, si alguna de las partes lo hubiese solicitado y el órgano jurisdiccional lo estimase pertinente, se celebrará una vista. El Tribunal podrá decidir

el alcance de las cuestiones sobre las que las partes deberán centrar sus alegaciones en dicha vista.

7. Finalizados los trámites mencionados en los tres apartados anteriores, el Tribunal competente adoptará en el plazo de diez días una de estas decisiones:

a) Si considerase que la decisión de la Comisión Europea es conforme al Derecho de la Unión Europea, dictará sentencia declarándolo así y denegando la autorización solicitada.

b) En caso de considerar que la decisión es contraria al Derecho de la Unión Europea, dictará auto de planteamiento de cuestión prejudicial de validez de la citada decisión ante el Tribunal de Justicia de la Unión Europea, en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea.

La autorización solamente podrá ser concedida si la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

8. El régimen de recursos será el previsto en esta ley.

[. . .]

§ 71

Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 186, de 5 de agosto de 1997
Última modificación: sin modificaciones
Referencia: BOE-A-1997-17574

Artículo 1. *Objeto.*

1. La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

Asimismo, esta norma establece específicamente el régimen de garantías de los derechos fundamentales y libertades públicas de los ciudadanos que habrá de respetarse ineludiblemente en las sucesivas fases de autorización, grabación y uso de las imágenes y sonidos obtenidos conjuntamente por las videocámaras.

2. Las referencias contenidas en esta Ley a videocámaras, cámaras fijas y cámaras móviles se entenderán hechas a cualquier medio técnico análogo y, en general, a cualquier sistema que permita las grabaciones previstas en esta Ley.

Artículo 2. *Ámbito de aplicación.*

1. La captación, reproducción y tratamiento de imágenes y sonidos, en los términos previstos en esta Ley, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo.

2. Sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

[. . .]

Artículo 8. *Conservación de las grabaciones.*

1. Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy

graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

2. Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas, siéndole de aplicación, en caso contrario, lo dispuesto en el artículo 10 de la presente Ley.

3. Se prohíbe la cesión o copia de las imágenes y sonidos obtenidos de conformidad con esta Ley, salvo en los supuestos previstos en el apartado 1 de este artículo.

4. Reglamentariamente la Administración competente determinará el órgano o autoridad gubernativa que tendrá a su cargo la custodia de las imágenes obtenidas y la responsabilidad sobre su ulterior destino, incluida su inutilización o destrucción. Dicho órgano será el competente para resolver sobre las peticiones de acceso o cancelación promovidas por los interesados.

[. . .]

Artículo 11. *Recursos.*

Contra las resoluciones dictadas en aplicación de lo previsto en esta Ley, cabrá la interposición de los recursos ordinarios en vía administrativa, contencioso-administrativa, así como los previstos en el artículo 53.2 de la Constitución, en los términos legalmente establecidos.

Disposición adicional primera.

Las Comunidades Autónomas con competencia para la protección de las personas y los bienes y para el mantenimiento del orden público, con arreglo a lo dispuesto en los correspondientes Estatutos de Autonomía, podrán dictar, con sujeción a lo prevenido en esta Ley, las disposiciones necesarias para regular y autorizar la utilización de videocámaras por sus fuerzas policiales y por las dependientes de las Corporaciones locales radicadas en su territorio, la custodia de las grabaciones obtenidas, la responsabilidad sobre su ulterior destino y las peticiones de acceso y cancelación de las mismas.

Cuando sean competentes para autorizar la utilización de videocámaras, las Comunidades Autónomas mencionadas en el párrafo anterior regularán la composición y el funcionamiento de la Comisión correspondiente, prevista en el artículo 3 de esta Ley, con especial sujeción a los principios de presidencia judicial y prohibición de mayoría de la Administración autorizante.

Disposición adicional segunda.

Cada autoridad competente para autorizar la instalación fija de videocámaras por parte de las Fuerzas y Cuerpos de Seguridad deberá crear un registro en el que consten todas las que haya autorizado.

[. . .]

Disposición adicional sexta.

Los propietarios y, en su caso, los titulares de derechos reales sobre los bienes afectados por las instalaciones reguladas en esta Ley, o quienes los posean por cualquier título, están obligados a facilitar y permitir su colocación y mantenimiento, sin perjuicio de la necesidad de obtener, en su caso, la autorización judicial prevista en el artículo 87.2 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y de las indemnizaciones que procedan según las leyes.

Disposición adicional séptima.

1. Se considerarán faltas muy graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado, las siguientes infracciones:

a) Alterar o manipular los registros de imágenes y sonidos siempre que no constituya delito.

b) Permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o utilizar éstos para fines distintos de los previstos legalmente.

c) Reproducir las imágenes y sonidos para fines distintos de los previstos en esta Ley.

d) Utilizar los medios técnicos regulados en esta Ley para fines distintos de los previstos en la misma.

2. Se considerarán faltas graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado las restantes infracciones a lo dispuesto en la presente Ley.

Disposición adicional octava.

La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el texto ar ticulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto legislativo 339/1990, de 2 de marzo, y demás normativa específica en la materia, y con sujeción a lo dispuesto en las Leyes Orgánicas 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, en el marco de los principios de utilización de las mismas previstos en esta Ley.

[. . .]

§ 72

Ley 14/1986, de 25 de abril, General de Sanidad. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 102, de 29 de abril de 1986
Última modificación: 23 de marzo de 2023
Referencia: BOE-A-1986-10499

[. . .]

TÍTULO VI

De la docencia y la investigación

[. . .]

CAPÍTULO II

Tratamiento de datos de la investigación en salud

Artículo ciento cinco bis.

El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

[. . .]

§ 73

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 157, de 2 de julio de 1985
Última modificación: 17 de febrero de 2025
Referencia: BOE-A-1985-12666

[. . .]

TÍTULO IV

De la composición y atribuciones de los órganos jurisdiccionales

CAPÍTULO I

Del Tribunal Supremo

[. . .]

Artículo 58.

La Sala de lo Contencioso-administrativo del Tribunal Supremo conocerá:

Primero. En única instancia, de los recursos contencioso-administrativos contra actos y disposiciones del Consejo de Ministros, de las Comisiones Delegadas del Gobierno y del Consejo General del Poder Judicial y contra los actos y disposiciones de los órganos competentes del Congreso de los Diputados y del Senado, del Tribunal Constitucional, del Tribunal de Cuentas y del Defensor del Pueblo en los términos y materias que la Ley establezca y de aquellos otros recursos que excepcionalmente le atribuya la ley.

Segundo. De los recursos de casación y revisión en los términos que establezca la ley.

Tercero. De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, cuando tal solicitud sea formulada por el Consejo General del Poder Judicial.

Cuarto. De la solicitud del Gobierno prevista en el artículo cuarto de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, para la convalidación o revocación de los acuerdos de asunción o intervención de la gestión directa del servicio o los de intervención o explotación de redes.

[. . .]

CAPÍTULO II

De la Audiencia Nacional

[. . .]

Artículo 66.

La Sala de lo Contencioso-Administrativo de la Audiencia Nacional conocerá:

a) En única instancia, de los recursos contencioso-administrativos contra disposiciones y actos de los Ministros, Ministras, Secretarios y Secretarias de Estado que la ley no atribuya a la Sección de lo Contencioso-Administrativo del Tribunal Central de Instancia.

b) En única instancia, de los recursos contencioso-administrativos contra los actos dictados por la Comisión de Vigilancia de Actividades de Financiación del Terrorismo. Conocerá, asimismo, de la posible prórroga de los plazos que le plantee dicha Comisión de Vigilancia respecto de las medidas previstas en los artículos 1 y 2 de la Ley 12/2003, de prevención y bloqueo de la financiación del terrorismo.

c) De los recursos devolutivos que la ley establezca contra las resoluciones de la Sección de lo Contencioso-Administrativo del Tribunal Central de Instancia.

d) De los recursos no atribuidos a los Tribunales Superiores de Justicia en relación a los convenios entre las Administraciones públicas y a las resoluciones del Tribunal Económico-Administrativo Central.

e) De las cuestiones de competencia que se puedan plantear entre los magistrados y magistradas de la Sección de lo Contencioso-Administrativo del Tribunal Central de Instancia y de aquellos otros recursos que excepcionalmente le atribuya la ley.

f) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la Agencia Española de Protección de Datos.

[. . .]

CAPÍTULO III

De los Tribunales Superiores de Justicia

[. . .]

Artículo 74.

1. Las Salas de lo Contencioso-Administrativo de los Tribunales Superiores de Justicia conocerán, en única instancia, de los recursos que se deduzcan en relación con:

a) Los actos de las Entidades locales y de las Administraciones de las comunidades autónomas, cuyo conocimiento no esté atribuido a las Secciones de lo Contencioso-Administrativo de los Tribunales de Instancia.

b) Las disposiciones generales emanadas de las comunidades autónomas y de las Entidades locales.

c) Los actos y disposiciones de los órganos de gobierno de las Asambleas legislativas de las comunidades autónomas y de las instituciones autonómicas análogas al Tribunal de Cuentas y al Defensor del Pueblo, en materia de personal, administración y gestión patrimonial.

d) Los actos y resoluciones dictados por los Tribunales Económico-Administrativos Regionales y Locales que pongan fin a la vía económico-administrativa.

e) Las resoluciones dictadas en alzada por el Tribunal Económico-Administrativo Central en materia de tributos cedidos.

f) Los actos y disposiciones de las Juntas Electorales Provinciales y de Comunidades Autónomas, así como los recursos contencioso-electorales contra acuerdos de las Juntas Electorales sobre proclamación de electos y elección y proclamación de Presidentes y Presidentas de Corporaciones locales en los términos de la legislación electoral.

g) Los convenios entre Administraciones públicas cuyas competencias se ejerzan en el ámbito territorial de la correspondiente comunidad autónoma.

h) La prohibición o la propuesta de modificación de reuniones previstas en la Ley Orgánica 9/1983, de 15 de julio, reguladora del derecho de reunión.

i) Los actos y resoluciones dictados por órganos de la Administración General del Estado cuya competencia se extienda a todo el territorio nacional y cuyo nivel orgánico sea inferior a Ministro, Ministra, Secretario o Secretaria de Estado, en materias de personal, propiedades especiales y expropiación forzosa, a excepción de lo dispuesto en el artículo 82.2. 3.º

j) Cualesquiera otras actuaciones administrativas no atribuidas expresamente a la competencia de otros órganos de este orden jurisdiccional.

k) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, cuando tal solicitud sea formulada por la autoridad de protección de datos de la comunidad autónoma respectiva.

2. Conocerán, en segunda instancia, de las apelaciones promovidas contra sentencias y autos dictados en las Secciones de lo Contencioso-Administrativo de los Tribunales de Instancia y de los correspondientes recursos de queja.

3. También les corresponde, con arreglo a lo establecido en esta ley, el conocimiento de los recursos de revisión contra las sentencias firmes dictadas en las Secciones de lo Contencioso-Administrativo de los Tribunales de Instancia.

4. Conocerán de las cuestiones de competencia entre las Secciones de lo Contencioso-Administrativo de los Tribunales de Instancia con sede en la comunidad autónoma.

5. Corresponde a las Salas de lo Contencioso-Administrativo de los Tribunales Superiores de Justicia autorizar, mediante auto, el requerimiento de información por parte de autoridades autonómicas de protección de datos a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.

[. . .]

CAPÍTULO V

De los Tribunales de Instancia y del Tribunal Central de Instancia

[. . .]

Artículo 90.

1. Con carácter general, en el Tribunal de Instancia, con sede en la capital de cada provincia y con jurisdicción en toda ella, existirá una Sección de lo Penal.

2. También podrán establecerse Secciones de lo Penal en Tribunales de Instancia que tengan su sede en poblaciones distintas de la capital de provincia, delimitándose en cada caso el ámbito territorial de su jurisdicción.

3. Las Secciones de lo Penal enjuiciarán las causas por delito que la ley determine.

A fin de facilitar el conocimiento de los asuntos instruidos por las Secciones de Violencia sobre la Mujer y las Secciones de Violencia contra la Infancia y la Adolescencia, y atendiendo al número de asuntos existentes, deberán especializarse una o varias plazas judiciales de la Sección de lo Penal, de conformidad con lo previsto en el artículo 96 de la presente ley.

4. Corresponde asimismo a las Secciones de lo Penal la ejecución de las sentencias dictadas en causas por delito grave o menos grave por las Secciones de Instrucción, Secciones de Violencia sobre la Mujer y Secciones de Violencia contra la Infancia y la Adolescencia; el reconocimiento y ejecución de las resoluciones que impongan sanciones pecuniarias transmitidas por las autoridades competentes de otros Estados miembros de la Unión Europea, cuando las mismas deban cumplirse en territorio español, y los procedimientos de decomiso autónomo por los delitos para cuyo conocimiento sean competentes.

5. Corresponde a las Secciones de lo Penal la emisión y la ejecución de los instrumentos de reconocimiento mutuo de resoluciones penales en la Unión Europea que les atribuya la ley.

[. . .]

TÍTULO III

De las actuaciones judiciales

CAPÍTULO I

De la oralidad, publicidad y lengua oficial

[. . .]

Artículo 235 ter.

1. Es público el acceso a los datos personales contenidos en los fallos de las sentencias firmes condenatorias, cuando se hubieren dictado en virtud de los delitos previstos en los siguientes artículos:

a) Los artículos 305, 305 bis y 306 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
b) Los artículos 257 y 258 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, cuando el acreedor defraudado hubiese sido la Hacienda Pública.
c) El artículo 2 de la Ley Orgánica 12/1995, de 12 de diciembre, de Represión del Contrabando, siempre que exista un perjuicio para la Hacienda Pública estatal o de la Unión Europea.

2. En los casos previstos en el apartado anterior, el Letrado de la Administración de Justicia emitirá certificado en el que se harán constar los siguientes datos:

a) Los que permitan la identificación del proceso judicial.
b) Nombre y apellidos o denominación social del condenado y, en su caso, del responsable civil.
c) Delito por el que se le hubiera condenado.
d) Las penas impuestas.
e) La cuantía correspondiente al perjuicio causado a la Hacienda Pública por todos los conceptos, según lo establecido en la sentencia.

Mediante diligencia de ordenación el Letrado de la Administración de Justicia ordenará su publicación en el "Boletín Oficial del Estado".
3. Lo dispuesto en este artículo no será de aplicación en el caso de que el condenado o, en su caso, el responsable civil, hubiera satisfecho o consignado en la cuenta de depósitos y consignaciones del órgano judicial competente la totalidad de la cuantía correspondiente al perjuicio causado a la Hacienda Pública por todos los conceptos, con anterioridad a la firmeza de la sentencia.

[. . .]

CAPÍTULO I BIS

Protección de datos de carácter personal en el ámbito de la Administración de Justicia

Artículo 236 bis.

1. El tratamiento de los datos personales podrá realizarse con fines jurisdiccionales o no jurisdiccionales. Tendrá fines jurisdiccionales el tratamiento de los datos que se encuentren incorporados a los procesos que tengan por finalidad el ejercicio de la actividad jurisdiccional.

2. El tratamiento de los datos personales en la Administración de Justicia se llevará cabo por el órgano competente y, dentro de él, por quien tenga la competencia atribuida por la normativa vigente.

Artículo 236 ter.

1. El tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo, sin perjuicio de las especialidades establecidas en el presente Capítulo y en las leyes procesales.

2. En el ámbito de la jurisdicción penal, el tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos, diligencias o expedientes de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en la Ley Orgánica de protección de datos personales tratados con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, sin perjuicio de las especialidades establecidas en el presente Capítulo y en las leyes procesales y, en su caso, en la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

3. No será necesario el consentimiento del interesado para que se proceda al tratamiento de los datos personales en el ejercicio de la actividad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba.

Artículo 236 quáter.

Cuando se proceda al tratamiento con fines no jurisdiccionales se estará a lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo.

Artículo 236 quinquies.

1. Las resoluciones y actuaciones procesales deberán contener los datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, en especial para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión.

2. Los Jueces y Magistrados, los Fiscales y los Letrados de la Administración de Justicia, conforme a sus competencias, podrán adoptar las medidas que sean necesarias para la supresión de los datos personales de las resoluciones y de los documentos a los que puedan acceder las partes durante la tramitación del proceso siempre que no sean necesarios para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión.

3. Los datos personales que las partes conocen a través del proceso deberán ser tratados por éstas de conformidad con la normativa general de protección de datos. Esta obligación también incumbe a los profesionales que representan y asisten a las partes, así como a cualquier otro que intervenga en el procedimiento.

4. Se deberán comunicar a los órganos competentes dependientes del Consejo General del Poder Judicial, de la Fiscalía General del Estado y del Ministerio de Justicia, en lo que proceda, los datos tratados con fines jurisdiccionales que sean estrictamente necesarios para el ejercicio de las funciones de inspección y control establecidas en esta Ley, y su normativa de desarrollo. También se deberán facilitar los datos tratados con fines no jurisdiccionales cuando ello esté justificado por la interposición de un recurso o sea necesario para el ejercicio de las competencias que tengan legalmente atribuidas.

5. Las Oficinas de Comunicación establecidas en esta Ley, en el ejercicio de sus funciones de comunicación institucional, deberán velar por el respeto del derecho fundamental a la protección de datos personales de aquellos que hubieran intervenido en el procedimiento de que se trate. Para cumplir con su finalidad, podrán recabar los datos necesarios de las autoridades competentes.

6. Los Letrados de la Administración de Justicia deberán facilitar a la Abogacía del Estado los datos personales, la información y los documentos que sean requeridos para el desempeño de la representación y defensa del Reino de España ante el Tribunal Europeo de Derechos Humanos y otros órganos internacionales en materia de protección de derechos Humanos, en particular ante el Comité de Naciones Unidas. A tales efectos, se establecerán igualmente los mecanismos de comunicación con la Fiscalía General del Estado, a través de sus unidades competentes.

Artículo 236 sexies.

1. La Administración competente deberá suministrar los medios tecnológicos adecuados para que se proceda al tratamiento de los datos personales conforme a las disposiciones legales y reglamentarias.

2. La Administración competente deberá cumplir con las responsabilidades que en materia de tratamiento y protección de datos personales se le atribuya como administración prestacional.

3. Se deberán adoptar las medidas organizativas adecuadas para que la Oficina judicial y fiscal realice un adecuado tratamiento de los datos personales. Previo informe del Consejo General del Poder judicial, y, en su caso, de la Fiscalía General del Estado, el Ministerio de Justicia deberá elaborar y actualizar los códigos de conducta destinados a contribuir a la correcta aplicación de la normativa de protección de datos personales en la Oficina judicial y fiscal, adecuando los principios de la normativa general a los propios de la regulación procesal y organización de la Oficina judicial y fiscal.

4. El Ministerio de Justicia y las Comunidades Autónomas con competencias en la materia, dentro de las políticas de apoyo a la Administración de Justicia y desarrollo de la gestión electrónica de los procedimientos, podrán realizar el tratamiento de datos no personales para el ejercicio de sus competencias de gestión pública, incluyendo el desarrollo e implementación de sistemas automáticos de clasificación documental orientados a la tramitación procesal, con cumplimiento de la normativa de interoperabilidad, seguridad y protección de datos que resulte aplicable.

Artículo 236 septies.

1. En relación con el tratamiento de los datos personales con fines jurisdiccionales, los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación al proceso en que los datos fueron recabados. Estos derechos deberán ejercitarse ante los órganos judiciales, fiscalías u Oficina judicial en los que se tramita el procedimiento, y las peticiones deberán resolverse por quien tenga la competencia atribuida en la normativa orgánica y procesal.

2. En todo caso se denegará el acceso a los datos objeto de tratamiento con fines jurisdiccionales cuando las diligencias procesales en que se haya recabado la información sean o hayan sido declaradas secretas o reservadas.

3. En relación con el tratamiento de los datos personales con fines no jurisdiccionales, los interesados podrán ejercitar los derechos de información, acceso, rectificación, supresión, oposición y limitación en los términos establecidos en la normativa general de protección de datos.

Artículo 236 octies.

1. Respecto a las operaciones de tratamiento efectuadas con fines jurisdiccionales por los Juzgados, Tribunales, Fiscalías, y las Oficinas judicial y fiscal, corresponderán al Consejo General del Poder Judicial y a la Fiscalía General del Estado, en el ámbito de sus respectivas competencias, las siguientes funciones:

a) Supervisar el cumplimiento de la normativa de protección de datos personales mediante el ejercicio de la labor inspectora otorgada en la presente Ley y el Estatuto Orgánico del Ministerio Fiscal.

b) Promover la sensibilización de los profesionales de la Administración de Justicia y su comprensión de los riesgos, normas, garantías, derechos y obligaciones en relación con el tratamiento.

c) Emitir informe sobre los códigos de conducta destinados a contribuir a la correcta aplicación de la normativa de protección de datos personales en la Oficina judicial y fiscal.

d) Previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en materia de protección de datos.

e) Tramitar y responder las reclamaciones presentadas por un interesado o por asociaciones, organizaciones y entidades que tengan capacidad procesal o legitimación para defender intereses colectivos, en los términos que determinen las leyes de aplicación al proceso en que los datos fueron recabados. Se informará al reclamante sobre el curso y resultado de la reclamación en un plazo razonable, previa realización de la investigación oportuna si se considera necesario.

2. Los tratamientos de datos con fines no jurisdiccionales estarán sometidos a la competencia de la Agencia Española de Protección de Datos, que también supervisará el cumplimiento de aquellos tratamientos que no sean competencia de las autoridades indicadas en el apartado anterior.

3. El Consejo General del Poder Judicial, la Fiscalía General del Estado y la Agencia Española de Protección de Datos colaborarán en aras del adecuado ejercicio de las respectivas competencias que la presente Ley Orgánica les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

4. Cuando con ocasión de la realización de actuaciones de investigación relacionadas con la posible comisión de una infracción de la normativa de protección de datos, las autoridades competentes a las que se refieran los apartados anteriores apreciasen la existencia de indicios que supongan la competencia de otra autoridad, darán inmediatamente traslado a esta última a fin de que prosiga con la tramitación del procedimiento.

Artículo 236 nonies.

Las competencias que corresponden al Consejo General del Poder Judicial como autoridad de protección de datos respecto del tratamiento de los mismos con fines jurisdiccionales por los tribunales se ejercerán por la Comisión de Supervisión y Control de Protección de Datos prevista en el artículo 610 ter. En el ejercicio de sus funciones la Comisión contará con el apoyo y la asistencia de la Dirección de Supervisión y Control de Protección de Datos, de acuerdo con lo previsto en el artículo 620 bis.

Artículo 236 decies.

1. Los tratamientos de datos llevados a cabo por el Consejo General del Poder judicial y la Fiscalía General del Estado en el ejercicio de sus competencias quedarán sometidos a lo dispuesto en la legislación vigente en materia de protección de datos personales. Dichos tratamientos no serán considerados en ningún caso realizados con fines jurisdiccionales.

2. Las operaciones de tratamiento de datos personales del Consejo General del Poder Judicial y de los órganos integrantes del mismo serán autorizados por acuerdo del Consejo General del Poder Judicial, a propuesta de la Secretaría General, que ostentará la condición de responsable del tratamiento respecto de los mismos.

3. Las operaciones de tratamiento de datos personales de la Fiscalía General del Estado serán autorizadas según determine el Estatuto Orgánico del Ministerio Fiscal y las Instrucciones que se dicten al respecto.

[. . .]

Artículo 434 bis.

Las Administraciones con competencias en materia de Justicia impulsarán la cooperación para garantizar la mejora continua en la Administración de Justicia fijando estándares de calidad homogéneos en todo el Estado.

A tal fin, y mediante convenios u otros instrumentos de colaboración y cooperación interadministrativa de los contemplados en la legislación vigente, se podrán articular estructuras para la definición, ejecución y seguimiento de proyectos compartidos entre las distintas Administraciones.

Con el mismo objetivo se establecerán cauces que permitan la participación de los Consejos Profesionales que desarrollan sus funciones, principalmente, en relación con la Administración de Justicia.

Se establece asimismo como objetivo prioritario de la cooperación establecer los medios materiales que permitan que el conjunto del procedimiento, las comunicaciones y actos de impulso procesal puedan desarrollarse íntegramente en todas las lenguas oficiales del Estado, garantizando así el respeto de los derechos lingüísticos de los ciudadanos.

Artículo 434 ter.

1. Se crea la Comisión para la Calidad del servicio público de Justicia que se encargará de elaborar con carácter anual un informe sobre la calidad del servicio público basado en datos. Este informe, entre otras cuestiones, valorará la eficiencia, la accesibilidad universal y la satisfacción del usuario o usuaria del sistema de Justicia, proponiendo a las Administraciones competentes aquellas mejoras normativas o de funcionamiento y de acceso a la Justicia para todas las personas, en condiciones de igualdad y no discriminación, que estime pertinentes, así como fijando objetivos anuales y estándares comunes y homogéneos que contribuyan a la mejora de la calidad del servicio público de Justicia. La Comisión desarrollará su trabajo en los ámbitos autonómico y estatal. Podrá desarrollar también su trabajo en el ámbito provincial a instancia de cualquiera de los miembros de la Comisión estatal o autonómica siempre que lo considere de utilidad en razón a los temas a tratar. En este caso, estará integrada por un miembro de cada una de las instituciones presentes en la Comisión autonómica y será convocada y presidida por el Presidente de la Audiencia Provincial.

2. Este órgano, para contribuir a la cogobernanza de la Administración de Justicia se estructura en comisiones autonómicas y en la Comisión estatal para la calidad del servicio público de Justicia; pudiendo funcionar en un ámbito provincial en el supuesto previsto en el apartado anterior.

3. La Comisión estatal estará integrada por una persona que represente a cada uno de los siguientes organismos e instituciones:

– Ministerio de Justicia.
– Consejo General del Poder Judicial.
– Cada una de las Comunidades Autónomas con competencias asumidas en materia de Justicia.
– Fiscalía General del Estado.
– Secretaría General de la Administración de Justicia.
– Consejo General de la Abogacía Española.
– Consejo General de Procuradores de los Tribunales de España.
– Consejo General de Graduados Sociales.
– Secretaría General del Comité técnico estatal de la Administración judicial electrónica.
– Organizaciones sindicales más representativas del personal al servicio de la Administración de Justicia, elegida por decisión mayoritaria entre ellas.

La Comisión estará presidida por el representante del Consejo General del Poder Judicial y por el representante del Ministerio de Justicia, por periodos anuales conforme a un turno rotatorio.

Corresponderá a la Presidencia la convocatoria de las reuniones y dirigir las sesiones.

4. Las Comisiones autonómicas estarán integradas por la Presidencia del Tribunal Superior o persona en quien delegue, que la presidirá, el Consejero o Consejera de Justicia de la Comunidad Autónoma en el caso de comunidades autónomas con competencias asumidas en materia de Administración de Justicia o persona en quien delegue, en otro caso, por un representante del Ministerio de Justicia, el o la Fiscal Jefe Superior o persona en quien delegue, el Secretario o Secretaria de Gobierno, un representante de los colegios de la abogacía del territorio y un representante de las organizaciones sindicales más representativas del personal al servicio de la Administración de Justicia de la comunidad autónoma elegido por decisión mayoritaria entre ellas.

5. Las Comisiones autonómicas se reunirán al menos una vez al trimestre para analizar el funcionamiento de los órganos judiciales de su ámbito territorial y elaborarán un informe al

respecto incluyendo las encuestas de satisfacción de las personas usuarias del servicio público, que se elevará a la Comisión estatal.

6. A las sesiones podrán acudir los técnicos que se consideren necesarios en función del orden del día prefijado.

CAPÍTULO II

De la oficina judicial

[. . .]

CAPÍTULO III

De las unidades administrativas

[. . .]

CAPÍTULO IV

De las Oficinas de Justicia en los municipios

Artículo 439 ter.

1. Las Oficinas de Justicia en los municipios son aquellas unidades que, sin estar integradas en la estructura de la Oficina judicial, se constituyen en el ámbito de la organización de la Administración de Justicia para la prestación de servicios a la ciudadanía de los respectivos municipios.

2. En cada municipio donde no tenga su sede un Tribunal de Instancia existirá una Oficina de Justicia, que prestará servicios en la localidad donde se encuentre ubicada. En ella el juez o jueza de paz dispondrá de recursos y espacios suficientes y adecuadamente señalizados.

3. Las instalaciones y medios instrumentales de estas Oficinas estarán a cargo del Ayuntamiento respectivo, salvo cuando fuere conveniente su gestión total o parcial por el Ministerio de Justicia o la comunidad autónoma con competencias asumidas en materia de Justicia. Los sistemas y equipos informáticos de las Oficinas serán facilitados por el Ministerio de Justicia o la comunidad autónoma respectiva en los casos que tengan asumidas las competencias en materia de Justicia.

4. Los Presupuestos Generales del Estado establecerán un crédito para subvencionar a los ayuntamientos por la atención de los conceptos regulados en el apartado anterior y, en su caso, del personal dependiente de este que preste servicio en estas Oficinas de Justicia. La subvención se modulará en función del número de habitantes de derecho del municipio. En las comunidades autónomas en las que se haya efectuado el traspaso de funciones de la Administración del Estado en materia de provisión de medios materiales y económicos para el funcionamiento de la Administración de Justicia, dicha subvención se dotará y librará por la correspondiente comunidad autónoma a los ayuntamientos de su respectivo territorio.

Artículo 439 quater.

1. En las Oficinas de Justicia en los municipios se prestarán los siguientes servicios:

a) La asistencia al juez o la jueza de paz del municipio en el ejercicio de las funciones que tenga atribuidas legalmente.

b) La práctica de los actos de comunicación procesal con quienes residan en el municipio o municipios para los que presten sus servicios, siempre que los mismos no se hayan podido practicar por medios electrónicos.

c) Los que, en su calidad de oficinas colaboradoras del Registro Civil, se establezcan en la ley o por vía reglamentaria.

2. Cuando el desarrollo de las herramientas informáticas y los medios materiales e instrumentales lo permitan, se prestarán también los siguientes:

a) La práctica de actuaciones procesales con residentes o personas que desarrollen su profesión o trabajo en el municipio, que deban llevarse a cabo mediante videoconferencia u otros sistemas de telepresencia incluida la intervención en actos de conciliación y derivados de expedientes de jurisdicción voluntaria.

b) La recepción de las solicitudes de reconocimiento del derecho a la asistencia jurídica gratuita y su remisión a los Colegios de la Abogacía encargados de su tramitación, así como las restantes actuaciones que puedan servir de apoyo a la gestión de estas solicitudes y su comunicación a los interesados.

c) Las solicitudes o gestión de peticiones de la ciudadanía, dirigidas a las Gerencias Territoriales del Ministerio de Justicia u órganos equivalentes en aquellas comunidades que tienen asumidas competencias en materia de Justicia.

d) La colaboración con las unidades de medios adecuados de solución de controversias existentes en su ámbito territorial, en coordinación con la Administración prestacional competente.

e) La colaboración con las Administraciones públicas competentes para que, en cuanto el desarrollo de las herramientas informáticas lo permita, se facilite a jueces, juezas, magistrados y magistradas, fiscales, letrados y letradas de la Administración de Justicia y al personal al servicio de la Administración de Justicia que no esté integrado en las relaciones de puestos de trabajo de dichas Oficinas, el desempeño ocasional de su actividad laboral en estas instalaciones, comunicando telemáticamente con sus respectivos puestos.

f) Aquellos otros servicios que figuren en convenios de colaboración entre diferentes Administraciones Públicas.

Artículo 439 quinquies.

1. Las Oficinas de Justicia de municipios de más de 7.000 habitantes y aquellas otras en las que la carga de trabajo lo justifique estarán servidas por funcionarios de los Cuerpos al servicio de la Administración de Justicia, y su determinación corresponderá al Ministerio de Justicia y a las comunidades autónomas con competencias asumidas, en sus respectivos ámbitos. En las respectivas relaciones de puestos de trabajo se podrán incluir determinados puestos a cubrir con personal de otras Administraciones Públicas, siempre que reúnan los requisitos y condiciones establecidas en aquéllas.

En todo caso, la Secretaría de estas Oficinas de Justicia será desempeñada por personal del Cuerpo de Gestión Procesal y Administrativa, conforme se determine en la correspondiente relación de puestos de trabajo.

2. El personal funcionario al servicio de la Administración de Justicia destinado en puestos de trabajo cuya actividad sea declarada compatible de conformidad con el artículo 521.3 E) realizará las tareas propias de la Oficina de Justicia en el municipio así como las de la Oficina judicial correspondiente. En el caso de estas últimas lo hará bajo la dependencia funcional del director o directora del servicio para el que desarrolle actividad compatible.

3. El Ministerio de Justicia o las comunidades autónomas con competencias en materia de Justicia, en sus respectivos ámbitos, podrán establecer agrupaciones de Oficinas de Justicia de municipios limítrofes de un mismo partido judicial para la prestación a la ciudadanía de los servicios a que se refiere el artículo anterior. En tales casos se determinará el municipio cabecera de la agrupación.

La Oficina de Justicia del municipio cabecera de agrupación deberá estar dotada con personal de la Administración de Justicia, quien prestará sus servicios en todas las Oficinas de Justicia de municipios integrados en la referida agrupación, conforme al régimen de atención que determinarán, en cada caso, el Ministerio de Justicia o las comunidades autónomas con competencias en materia de Justicia.

Para la atención en las Oficinas de Justicia de los municipios integradas en las referidas agrupaciones que no estén dotadas con personal de la Administración de Justicia, los ayuntamientos nombrarán personal funcionario, laboral o, en defecto de ambos, persona idónea para auxiliar al personal de los Cuerpos al servicio de la Administración de Justicia en la prestación de los servicios en ese municipio. Los requisitos de idoneidad que deberá reunir la persona que no tenga la condición de funcionario público vendrán establecidos en la propia norma en que se constituyan las referidas agrupaciones. En todo caso, la designación deberá recaer en personas mayores de edad que no estén incursas en causas que impidan

el ejercicio de un cargo público. El auxilio que preste este personal no comprenderá aquellas actuaciones cuya ejecución esté reservada al personal de la Administración de Justicia.

CAPÍTULO V

De la oficina fiscal

Artículo 439 sexies.

1. La Oficina fiscal es la organización de carácter instrumental que sirve de soporte y apoyo a la actividad del Ministerio Fiscal.

2. La estructura básica de la Oficina fiscal, que podrá dividirse en áreas y equipos, será homogénea en todo el territorio del Estado y estará basada en los principios de jerarquía, división de funciones y coordinación.

3. La Oficina fiscal funcionará con criterios de agilidad, eficacia, eficiencia, racionalización del trabajo, responsabilidad por la gestión, coordinación y cooperación entre Administraciones, de manera que los ciudadanos obtengan un servicio próximo y de calidad, con respeto a los principios recogidos en la Carta de Derechos de los ciudadanos ante la Justicia.

4. Los puestos de trabajo de la Oficina fiscal solo podrán ser cubiertos por personal de los cuerpos de funcionarios al servicio de la Administración de Justicia, y se ordenarán de acuerdo con lo establecido en las relaciones de puestos de trabajo.

El personal que presta sus servicios en las oficinas fiscales, sin perjuicio de su dependencia funcional, depende orgánicamente del Ministerio de Justicia o de las Comunidades Autónomas con competencias asumidas en sus respectivos ámbitos.

[. . .]

LIBRO VIII

Del Consejo General del Poder Judicial

TÍTULO I

De las atribuciones del Consejo General del Poder Judicial

[. . .]

Artículo 560.

1. El Consejo General del Poder Judicial tiene las siguientes atribuciones:

1.ª Proponer el nombramiento, en los términos previstos por la presente Ley Orgánica, del Presidente del Tribunal Supremo y del Consejo General del Poder Judicial.

2.ª Proponer el nombramiento de Jueces, Magistrados y Magistrados del Tribunal Supremo.

3.ª Proponer el nombramiento, en los términos previstos por la presente Ley Orgánica, de dos Magistrados del Tribunal Constitucional.

4.ª Ser oído por el Gobierno antes del nombramiento del Fiscal General del Estado.

5.ª Interponer el conflicto de atribuciones entre órganos constitucionales del Estado, en los términos previstos por la Ley Orgánica del Tribunal Constitucional.

6.ª Participar, en los términos legalmente previstos, en la selección de Jueces y Magistrados.

7.ª Resolver lo que proceda en materia de formación y perfeccionamiento, provisión de destinos, ascensos, situaciones administrativas y régimen disciplinario de Jueces y Magistrados.

8.ª Ejercer la alta inspección de Tribunales, así como la supervisión y coordinación de la actividad inspectora ordinaria de los Presidentes y Salas de Gobierno de los Tribunales.

9.ª Impartir instrucciones a los órganos de gobierno de Juzgados y Tribunales en materias de la competencia de éstos, así como resolver los recursos de alzada que se interpongan contra cualesquiera acuerdos de los mismos.

10.ª Cuidar de la publicación oficial de las sentencias y demás resoluciones que se determinen del Tribunal Supremo y del resto de órganos judiciales.

A tal efecto el Consejo General del Poder Judicial, previo informe de las Administraciones competentes, establecerá reglamentariamente el modo en que se realizará la recopilación de las sentencias, su tratamiento, difusión y certificación, para velar por su integridad, autenticidad y acceso, así como para asegurar el cumplimiento de la legislación en materia de protección de datos personales.

11.ª Regular la estructura y funcionamiento de la Escuela Judicial, así como nombrar a su Director y a sus profesores.

12.ª Regular la estructura y funcionamiento del Centro de Documentación Judicial, así como nombrar a su Director y al resto de su personal.

13.ª Nombrar al Vicepresidente del Tribunal Supremo, al Promotor de la Acción Disciplinaria y al Jefe de la Inspección de Tribunales.

14.ª Nombrar al Director del Gabinete Técnico del Consejo General del Poder Judicial.

15.ª Regular y convocar el concurso-oposición de ingreso en el Cuerpo de Letrados del Consejo General del Poder Judicial.

16.ª Ejercer la potestad reglamentaria, en el marco estricto de desarrollo de las previsiones de la Ley Orgánica del Poder Judicial, en las siguientes materias:

a) Organización y funcionamiento del Consejo General del Poder Judicial.

b) Personal del Consejo General del Poder Judicial en el marco de la legislación sobre la función pública.

c) Órganos de gobierno de Juzgados y Tribunales.

d) Publicidad de las actuaciones judiciales.

e) Publicación y reutilización de las resoluciones judiciales.

f) Habilitación de días y horas, así como fijación de horas de audiencia pública.

g) Constitución de los órganos judiciales fuera de su sede.

h) Especialización de órganos judiciales.

i) Reparto de asuntos y ponencias.

j) Régimen de guardias de los órganos jurisdiccionales.

k) Organización y gestión de la actuación de los órganos judiciales españoles en materia de cooperación jurisdiccional interna e internacional.

l) **(Suprimida)**

m) Condiciones accesorias para el ejercicio de los derechos y deberes que conforman el estatuto de Jueces y Magistrados, así como el régimen jurídico de las Asociaciones judiciales, sin que tal desarrollo reglamentario pueda suponer innovación o alteración alguna de la regulación legal.

En ningún caso, las disposiciones reglamentarias del Consejo General del Poder Judicial podrán afectar o regular directa o indirectamente los derechos y deberes de personas ajenas al mismo.

17.ª Elaborar y ejecutar su propio presupuesto, en los términos previstos en la presente Ley Orgánica.

18.ª Aprobar la relación de puestos de trabajo del personal funcionario a su servicio.

19ª En materia de protección de datos personales, ejercerá las funciones definidas en el artículo 236 octies.

20.ª Recibir quejas de los ciudadanos en materias relacionadas con la Administración de Justicia.

21.ª Elaborar y aprobar, conjuntamente con el Ministerio de Justicia y, en su caso, oídas las Comunidades Autónomas cuando afectare a materias de su competencia, los sistemas de racionalización, organización y medición de trabajo que se estimen convenientes para determinar la carga de trabajo que pueda soportar un órgano jurisdiccional.

La determinación de la carga de trabajo que cabe exigir, a efectos disciplinarios, al Juez o Magistrado corresponderá en exclusiva al Consejo General del Poder Judicial.

22.ª Proponer, previa justificación de la necesidad, las medidas de refuerzo que sean precisas en concretos órganos judiciales.

23.ª Emitir informe en los expedientes de responsabilidad patrimonial por anormal funcionamiento de la Administración de Justicia.

24.ª La recopilación y actualización de los Principios de Ética Judicial y su divulgación, así como su promoción con otras entidades y organizaciones judiciales, nacionales o internacionales.

El asesoramiento especializado a los jueces y magistrados en materia de conflictos de intereses, así como en las demás materias relacionadas con la integridad.

El Consejo General del Poder Judicial se asegurará de que la Comisión de Ética Judicial, que a tal efecto se constituya, esté dotada de los recursos y medios adecuados para el cumplimiento de sus objetivos.

25.ª Aquellas otras que le atribuya la Ley Orgánica del Poder Judicial.

2. Los proyectos de reglamentos de desarrollo se someterán a informe de las asociaciones profesionales de Jueces y Magistrados y de las corporaciones profesionales o asociaciones de otra naturaleza que tengan reconocida legalmente representación de intereses a los que puedan afectar. Se dará intervención a la Administración del Estado, por medio del Ministerio de Justicia, y a las de las Comunidades Autónomas siempre que una y otras tengan competencias relacionadas con el contenido del reglamento o sea necesario coordinar éstas con las del Consejo General. Se recabarán las consultas y los estudios previos que se consideren pertinentes y un dictamen de legalidad sobre el proyecto.

En todo caso, se elaborará un informe previo de impacto de género.

El Ministerio Fiscal será oído cuando le afecte la materia sobre la que verse el proyecto y especialmente en los supuestos contemplados en las letras d) y f) a j) del apartado 1.16.ª de este artículo.

3. **(Suprimido)**

4. Cuando en el ejercicio de las atribuciones legalmente previstas en este artículo el Consejo General del Poder Judicial adopte medidas que comporten un incremento de gasto, será preciso informe favorable de la Administración competente que deba soportar dicho gasto.

[. . .]

CAPÍTULO VIII

La Comisión de Supervisión y Control de Protección de Datos

Artículo 610 ter.

1. El Pleno del Consejo General del Poder Judicial elegirá de entre sus Vocales a los integrantes de la Comisión de Supervisión y Control de Protección de Datos por un mandato de cinco años y designará, entre ellos, a su Presidente o Presidenta.

2. La Comisión de Supervisión y Control de Protección de Datos estará integrada por tres Vocales, dos de ellos del turno judicial y uno de ellos del turno de juristas de reconocida competencia.

3. La Comisión de Supervisión y Control de Protección de Datos deberá actuar con la asistencia de todos sus componentes.

4. Corresponderá a la Comisión de Supervisión y Control de Protección de Datos el ejercicio de las funciones previstas en el artículo 236 octies en relación con los tratamientos de datos personales con fines jurisdiccionales realizados por tribunales. Sus acuerdos agotarán la vía administrativa y contra ellos cabrá interponer recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo del Tribunal Supremo. El conocimiento de estos recursos corresponderá a la sección prevista en el artículo 638.2.

5. Los Vocales integrantes de la Comisión estarán sujetos al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las

informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones.

[. . .]

Sección 7.ª La Dirección de Supervisión y Control de Protección de Datos

Artículo 620 bis.

1. La Dirección de Supervisión y Control de Protección de Datos es el órgano técnico del Consejo General del Poder Judicial encargado del apoyo y la asistencia a la Comisión de Supervisión y Control de Protección de Datos en el ejercicio de sus funciones.

2. La persona titular de la Dirección de Supervisión y Control de Protección de Datos será nombrada por el Pleno del Consejo General del Poder Judicial entre juristas de reconocida competencia con al menos quince años de ejercicio profesional y con conocimientos y experiencia acreditados en materia de protección de datos.

3. La persona titular de la Dirección de Supervisión y Control de Protección de Datos, que ejercerá sus funciones únicamente sujeta a las orientaciones, indicaciones e instrucciones de la Comisión de Supervisión y Control de Protección de Datos, estará sometida al mismo régimen jurídico en materia de situaciones administrativas, incompatibilidades, duración del mandato y retribuciones que el aplicable a los letrados del Consejo General del Poder Judicial. La persona titular de esta Dirección y el resto del personal adscrito a la misma estarán sujetos al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o en el ejercicio de sus atribuciones. Este deber de secreto profesional se aplicará en particular a la información que faciliten las personas físicas a la Dirección de Supervisión y Control de Protección de Datos en materia de infracciones de la normativa de protección de datos.

4. El Consejo General del Poder Judicial velará porque la Dirección de Supervisión y Control de Protección de Datos cuente, en todo caso, con todos los medios personales y materiales necesarios para el adecuado ejercicio de sus funciones.

5. Reglamentariamente se desarrollará la composición, organización y funcionamiento de la Dirección de Supervisión y Control de Protección de Datos.

[. . .]

§ 74

Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 147, de 20 de junio de 1985
Última modificación: 3 de enero de 2025
Referencia: BOE-A-1985-11672

[. . .]

TÍTULO PRIMERO

Disposiciones comunes para las elecciones por sufragio universal directo

[. . .]

CAPÍTULO IV

El censo electoral

[. . .]

Sección III. Rectificación del censo en período electoral

Artículo treinta y nueve. *Rectificación del Censo en período electoral.*

1. Para cada elección el Censo Electoral vigente será el cerrado el día primero del segundo mes anterior a la convocatoria.

2. Los ayuntamientos y consulados estarán obligados a mantener un servicio de consulta de las listas electorales vigentes de sus respectivos municipios y demarcaciones durante el plazo de ocho días, a partir del sexto día posterior a la convocatoria de elecciones.

La consulta podrá realizarse por medios informáticos, previa identificación del interesado, o mediante la exposición al público de las listas electorales, si no se cuenta con medios informáticos suficientes para ello.

3. Dentro del plazo anterior, cualquier persona podrá formular reclamación dirigida a la Delegación Provincial de la Oficina del Censo Electoral sobre sus datos censales, si bien solo podrán ser tenidas en cuenta las que se refieran a la rectificación de errores en los datos personales, a los cambios de domicilio dentro de una misma circunscripción o a la no inclusión del reclamante en ninguna Sección del Censo de la circunscripción pese a tener derecho a ello. También serán atendidas las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral. No serán tenidas en cuenta para la elección convocada las que reflejen un cambio de residencia de una

circunscripción a otra, realizado con posterioridad a la fecha de cierre del censo para cada elección, debiendo ejercer su derecho en la sección correspondiente a su domicilio anterior.

4. También en el mismo plazo los representantes de las candidaturas podrán impugnar el censo de las circunscripciones que en los seis meses anteriores hayan registrado un incremento de residentes significativo y no justificado que haya dado lugar a la comunicación a que se refiere el artículo 30.c).

5. Las reclamaciones podrán presentarse directamente en las delegaciones provinciales de la Oficina del Censo Electoral correspondiente o a través de los ayuntamientos o consulados, quienes las remitirán inmediatamente a las respectivas Delegaciones.

6. La Delegación Provincial de la Oficina del Censo Electoral, en un plazo de tres días, resolverá las reclamaciones presentadas y ordenará las rectificaciones pertinentes, que habrán de ser expuestas al público el décimo séptimo día posterior a la convocatoria. Asimismo se notificará la resolución adoptada a cada uno de los reclamantes y a los Ayuntamientos y Consulados correspondientes.

7. La Oficina del Censo Electoral remitirá a todos los electores una tarjeta censal con los datos actualizados de su inscripción en el censo electoral y de la Sección y Mesa en la que le corresponde votar, y comunicará igualmente a los electores afectados las modificaciones de Secciones, locales o Mesas, a que se refiere el artículo 24 de la presente Ley Orgánica.

[. . .]

Sección IV. Acceso a los datos censales

Artículo cuarenta y uno.

1. Por real decreto se regularán los datos personales de los electores, necesarios para su inscripción en el censo electoral, así como los de las listas y copias del censo electoral.

2. Queda prohibida cualquier información particularizada sobre los datos personales contenidos en el censo electoral, a excepción de los que se soliciten por conducto judicial.

3. No obstante, la Oficina del Censo Electoral puede facilitar datos estadísticos que no revelen circunstancias personales de los electores.

4. Las comunidades autónomas podrán obtener una copia del censo, en soporte apto para su tratamiento informático, después de cada convocatoria electoral, además de la correspondiente rectificación de aquél.

5. Los representantes de cada candidatura podrán obtener dentro de los dos días siguientes a la proclamación de su candidatura una copia del censo del distrito correspondiente, ordenado por mesas, en soporte apto para su tratamiento informático, que podrá ser utilizado exclusivamente para los fines previstos en la presente Ley. Alternativamente los representantes generales podrán obtener en las mismas condiciones una copia del censo vigente de los distritos donde su partido, federación o coalición presente candidaturas. Asimismo, las Juntas Electorales de Zona dispondrán de una copia del censo electoral utilizable, correspondiente a su ámbito.

Las Juntas Electorales, mediante resolución motivada, podrán suspender cautelarmente la entrega de las copias del censo a los representantes antes citados cuando la proclamación de sus candidaturas haya sido objeto de recurso o cuando se considere que podrían estar incursas en alguna de las circunstancias previstas en el artículo 44.4 de esta Ley.

6. Excepcionalmente y por razones debidamente justificadas, podrá excluirse a las personas que pudieran ser objeto de amenazas o coacciones que pongan en peligro su vida, su integridad física o su libertad, de las copias del censo electoral a que se refiere el apartado 5 del presente artículo.

[. . .]

CAPÍTULO VI

Procedimiento electoral

[. . .]

Sección V. Propaganda y actos de campaña electoral

[. . .]

Artículo cincuenta y ocho bis. *Utilización de medios tecnológicos y datos personales en las actividades electorales.*

1. **(Anulado)**

2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.

[. . .]

§ 75

Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 31, de 5 de febrero de 2020
Última modificación: 27 de abril de 2024
Referencia: BOE-A-2020-1651

[. . .]

LIBRO SEGUNDO

Medidas para la adaptación del derecho español a la normativa de la Unión Europea en materia de seguros privados y planes y fondos de pensiones

TÍTULO I

Transposición de la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros

[. . .]

CAPÍTULO III

De las actividades de los distribuidores de seguros y de reaseguros residentes o domiciliados en España

[. . .]

Sección 7.ª Competencias de ordenación y supervisión

[. . .]

Subsección 3.ª Protección de datos de carácter personal

Artículo 203. *Condición de responsable o encargado del tratamiento.*

1. A los efectos previstos en la Ley Orgánica 3/2018, de 5 de diciembre, así como en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016,

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos:

a) Los agentes de seguros y los operadores de banca-seguros tendrán la condición de encargados del tratamiento de la entidad aseguradora con la que hubieran celebrado el correspondiente contrato de agencia, en los términos previstos en el título I.

b) Los corredores de seguros y los corredores de reaseguros tendrán la condición de responsables del tratamiento respecto de los datos de las personas que acudan a ellos.

c) Los colaboradores externos a los que se refiere el artículo 137 tendrán la condición de encargados del tratamiento de los agentes o corredores de seguros con los que hubieran celebrado el correspondiente contrato mercantil. En este caso, solo podrán tratar los datos para los fines previstos en el artículo 137.1.

2. En el supuesto previsto en la letra a) del apartado 1, en el contrato de agencia deberán hacerse constar los extremos previstos en el artículo 28.3 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Del mismo modo, en el supuesto previsto en el apartado 1.c) deberán incluirse en el contrato mercantil celebrado con los colaboradores externos los extremos previstos en el artículo 28.3 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

3. Las entidades aseguradoras no podrán conservar los datos que les faciliten los mediadores de seguros, y que no deriven en la celebración de un contrato de seguro, estando obligadas a eliminarlos salvo que exista otra base jurídica que permita un tratamiento legítimo de los datos conforme al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Artículo 204. *Otras normas de protección de datos.*

1. En la publicidad que remitan a terceros los mediadores de seguros y reaseguros, a través de comunicaciones electrónicas, deberá estarse a lo dispuesto en los artículos 21 y 22.1 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

2. Los agentes de seguros y operadores de banca-seguros únicamente podrán tratar los datos de los interesados en los términos y con el alcance que se desprenda del contrato de agencia de seguros y siempre en nombre y por cuenta de la entidad aseguradora con la que hubieran celebrado el contrato.

Los operadores de banca-seguros no podrán tratar los datos relacionados con su actividad mediadora para fines propios de su objeto social sin contar con el consentimiento inequívoco y específico de los afectados.

3. Los corredores de seguros podrán tratar los datos de las personas que se dirijan a ellos amparándose en alguno de los supuestos del artículo 6.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

4. Resuelto el contrato de seguro en cuya distribución hubiera intervenido un corredor de seguros o un corredor de reaseguros, este deberá proceder a la cancelación de los datos, a menos que el interesado le hubiera autorizado el tratamiento de los mismos para otras finalidades y, en particular, para la celebración de un nuevo contrato.

En todo caso, el corredor de seguros y el corredor de reaseguros no podrán facilitar los datos del interesado a otra entidad distinta de aquella con la que el interesado hubiera celebrado el contrato resuelto si no media su consentimiento inequívoco para ello.

5. El tratamiento de los datos que los distribuidores de seguros lleven a cabo para valorar la honorabilidad comercial y profesional en el marco de lo dispuesto en el título I, deberá limitarse a la exclusiva finalidad de suministro de la información a la Dirección General de Seguros y Fondos de Pensiones, quedando expresamente limitado el número de personas que dentro de la organización pueda tener acceso a dichos datos.

[. . .]

§ 76

Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves

Jefatura del Estado
«BOE» núm. 248, de 17 de septiembre de 2020
Última modificación: 27 de mayo de 2021
Referencia: BOE-A-2020-10776

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

PREÁMBULO

I

La protección de la vida y de la seguridad de los ciudadanos constituye el objetivo principal del espacio de libertad, seguridad y justicia de la Unión Europea. Entre las medidas que se han adoptado para su consecución, el Consejo de la Unión Europea, a través del «Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano», de 4 de mayo de 2010, instó a la Comisión a presentar una propuesta sobre la utilización de datos del Registro de Nombres de los Pasajeros («Passenger Name Record», en adelante PNR) para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves.

Asimismo, en el plano internacional se ha venido avanzando en la dimensión exterior de esta política de la Unión Europea. La Comisión presentó una serie de elementos esenciales de la misma en su Comunicación de 21 de septiembre de 2010 «Sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países», y la Unión alcanzó diversos acuerdos internacionales con distintos Estados.

El incremento de la amenaza del crimen organizado y especialmente del terrorismo en Europa constituyen violaciones muy graves de los valores universales de la dignidad humana, la libertad, la igualdad, la solidaridad y el disfrute de los derechos humanos y de la libertades fundamentales en los que se basa la Unión Europea. Con el objetivo de elevar los niveles de seguridad de sus ciudadanos y de crear un marco jurídico para la protección de

sus datos de carácter personal, en lo que respecta a su tratamiento por las autoridades competentes, se adoptó la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del Registro de Nombres de los Pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

Con este fin se insta a los Estados miembros a que introduzcan en sus ordenamientos internos las disposiciones legales pertinentes para que los datos PNR de los vuelos exteriores de la Unión Europea sean transferidos a una Unidad de Información sobre Pasajeros que se cree en cada Estado, sin perjuicio de que pueda también aplicarse a los vuelos interiores de la Unión, según el criterio de cada país, como prevé la aludida Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, posibilidad de la que se hace uso en esta ley orgánica.

Asimismo, la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, exige la creación de un sistema uniforme en la Unión Europea para el tratamiento de los datos PNR, precisando claramente cuáles son estos, los fines a los que se limita su recogida, la utilización y transmisión, el establecimiento de unidades únicas de información sobre los pasajeros en cada Estado miembro, así como la obligatoriedad de la adopción de medidas que faciliten el cumplimiento por los operadores de sus deberes, incluida la imposición de sanciones efectivas, proporcionadas y disuasorias ante eventuales incumplimientos.

El tratamiento de los datos PNR va a mejorar la respuesta a la amenaza del terrorismo y la delincuencia grave mediante el cotejo de tales datos con las bases de datos disponibles y pertinentes, a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, y el análisis y evaluación de los mismos utilizando unos criterios específicos y revisables periódicamente, que permitan la identificación de personas que pudieran estar relacionadas con este tipo de actividades criminales, al tiempo que minimizarán al máximo el riesgo de afectar a personas inocentes.

II

Esta ley orgánica se estructura en tres capítulos, treinta y cuatro artículos, seis disposiciones adicionales y cuatro disposiciones finales.

El capítulo I establece las disposiciones generales.

Su objeto es regular, por un lado la transferencia de los datos PNR por parte de las compañías aéreas y otras entidades obligadas; en segundo término, la recogida, el tratamiento y la protección de esos datos, su transmisión a las autoridades competentes y el intercambio de dichos datos con otros Estados miembros, Europol y terceros Estados; a su vez, la designación de la Unidad de Información sobre Pasajeros española, y por último, el régimen sancionador.

Se especifican los fines para los que pueden ser utilizados los datos PNR, únicamente para prevenir, detectar, investigar y enjuiciar delitos de terrorismo y delitos graves.

El ámbito de aplicación contempla, en principio, todos los vuelos internacionales que tengan origen, destino o tránsito en España, tanto de carácter comercial como privados, con una serie de excepciones basadas en el tipo de los vuelos.

Excepcionalmente, como medida extraordinaria y siempre que existan indicios suficientes de una contrastada situación de riesgo, se podrán sujetar rutas o vuelos concretos de ámbito nacional a lo dispuesto en esta ley orgánica.

Asimismo, se definen los sujetos obligados, diferenciando las compañías áreas de las entidades de gestión de reservas de vuelos, cuya incorporación en esta ley orgánica es una posibilidad prevista en Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Se determinan también los delitos de terrorismo y los demás delitos graves cuya prevención, detección, investigación o enjuiciamiento justifica la recogida de los datos PNR. Los delitos de terrorismo son los contemplados en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, como delitos de las organizaciones y grupos terroristas y delitos de terrorismo. En cuanto a los demás delitos graves, se considera como tales, a los efectos de esta ley, aquellos castigados con una pena de prisión igual o superior a tres años

por ser constitutivos de algunos de los enumerados en el anexo II de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Por otro lado, se especifican los datos de los pasajeros que deben ser enviados a la Unidad de Información sobre Pasajeros, de entre los recopilados por parte de los sujetos obligados para sus propios fines comerciales en el transcurso normal de su actividad. Entre estos figuran los datos contenidos en el sistema de información anticipada sobre pasajeros (sistema API), algunos de los cuales, a diferencia de los anteriores, han sido contrastados con los documentos oficiales de identificación.

Deberá enviarse también cierta información sobre la tripulación correspondiente a los datos API. Asimismo, en el caso de los vuelos privados se deberán enviar dichos datos tanto de los pasajeros como de los tripulantes. Es imprescindible, para la consecución de las finalidades previstas en la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, disponer de tales datos de tripulaciones y de vuelos privados, sin los cuales se podrían correr graves riesgos de seguridad pública, como ha demostrado la experiencia de los últimos años.

El capítulo II se ocupa del tratamiento de los datos PNR.

Se regula la Unidad de Información sobre Pasajeros española (UIP), incardinada en la estructura del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado dependiente de la Secretaría de Estado de Seguridad, órgano con experiencia en materia de coordinación y en la recepción y análisis de la información estratégica disponible en la lucha contra todo tipo de terrorismo y delincuencia organizada.

Se determinan sus funciones, referidas tanto a la recepción, tratamiento y análisis de los datos PNR, como a las comunicaciones e intercambios de estos con las autoridades competentes nacionales y unidades análogas de otros Estados miembros, terceros países y Europol.

Se regula específicamente la figura del responsable de protección de datos, cuyo principal cometido será el de garantizar la rigurosa observancia de la legislación vigente en materia de protección de datos de carácter personal durante todo el proceso de recepción, tratamiento, transmisión, conservación y supresión de los datos PNR.

La transmisión de datos se llevará a cabo utilizando los formatos determinados y los protocolos definidos en la Decisión de Ejecución de la Comisión UE 2017/759, de 28 de abril de 2017, relativa a los protocolos comunes y los formatos de datos que deberán utilizar las compañías aéreas para la transmisión de los datos PNR a las Unidades de Información sobre Pasajeros.

Las compañías aéreas informarán a la UIP del formato y protocolo de transmisión que utilizarán. Con respecto a las compañías aéreas que no dispongan de la infraestructura técnica necesaria, se contempla la posibilidad de acordar con el Ministerio del Interior los medios electrónicos de transmisión, siempre que se respeten las garantías de seguridad.

Los datos serán enviados en dos momentos distintos; el primero entre las cuarenta y ocho y las veinticuatro horas anteriores a la salida programada del vuelo, y el segundo se producirá una vez cerrado el vuelo, es decir, en el momento a partir del cual nadie puede entrar en el avión ni abandonarlo. Si durante el vuelo se produce alguna modificación en el destino, también deberá ser transmitida.

Cuando sea necesario acceder a los datos PNR para responder a una amenaza real y concreta en momentos distintos a los anteriores, caso por caso, las compañías aéreas deberán transmitir a la UIP dichos datos con carácter inmediato al requerimiento recibido.

Sin perjuicio de las obligaciones establecidas en esta ley orgánica, los tratamientos de datos de carácter personal realizados por los sujetos obligados se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por la legislación interna que se dicte en uso de la habilitación contenida en aquel.

En relación con el tratamiento de los datos de carácter personal por parte de las autoridades competentes, estas estarán sujetas al deber de proporcionar o poner a disposición del interesado la información y facilitar el ejercicio de los derechos de estos contemplados en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la ley orgánica que la incorpore a nuestro ordenamiento interno.

En este capítulo también se definen los propósitos para los que la UIP realizará el tratamiento de los datos PNR mediante la utilización de una definida metodología: Evaluar a las personas a bordo de la aeronave a fin de identificar a aquellas que pudieran tener relación con delitos de terrorismo o delitos graves; revisar individualmente los resultados de dicha evaluación previa automatizada; responder peticiones de las autoridades competentes o de Europol y establecer criterios predeterminados a utilizar en esas evaluaciones.

Para ello, la UIP cotejará los datos PNR con las bases de datos disponibles y pertinentes a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, y tratará los datos de acuerdo con los criterios predeterminados. Se realizará una verificación automática a priori, que, en el caso de ofrecer un resultado positivo, requerirá necesariamente una comprobación manual por parte de un especialista de la propia UIP.

Se precisa cuáles son las autoridades competentes que pueden solicitar o recibir datos PNR o el resultado del tratamiento de dichos datos por la UIP, con el objetivo de seguir examinando dicha información o adoptar las medidas adecuadas para prevenir, detectar, investigar y enjuiciar delitos de terrorismo y delitos graves. Estas son las Direcciones Generales de la Policía y de la Guardia Civil, el Centro Nacional de Inteligencia, la Dirección Adjunta de Vigilancia Aduanera y el Ministerio Fiscal. También se contemplan como autoridades competentes las correspondientes de las Comunidades Autónomas que hayan asumido estatutariamente competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana y cuenten con un cuerpo de policía propio. Los Jueces y Tribunales, en garantía del principio de independencia constitucional, se regirán en cuanto a las peticiones de dicha información y a la colaboración con la UIP por lo dispuesto en su legislación específica.

Las peticiones de las autoridades competentes serán debidamente motivadas y con suficiente base. En ningún caso se admitirán peticiones masivas y no fundamentadas. Todo tratamiento que lleven a cabo estas autoridades competentes sobre los datos recibidos de la UIP, lo será para los fines propios de la lucha contra los delitos de terrorismo y los delitos graves.

El capítulo recoge, además, una serie de disposiciones en materia de protección de datos, entre las que figuran la obligación de conservación de la documentación relativa a los sistemas y procedimientos de tratamiento; la obligación de registro de las operaciones de recogida, consulta, transferencia y supresión de los datos, así como la obligación de comunicar al interesado y a la autoridad nacional de control cualquier violación de los datos personales que dé lugar a un elevado riesgo para la protección de los mismos o afecte negativamente a la intimidad del interesado.

En una Europa concebida como espacio de libertad, seguridad y justicia, la colaboración y cooperación entre los Estados miembros cobra una especial relevancia. Y dentro de esa cooperación, los aspectos relativos a la seguridad se han tornado fundamentales en los últimos años en la lucha contra el terrorismo y la criminalidad organizada. En esa línea de colaboración, España podrá enviar datos PNR o el resultado de su tratamiento a otros Estados miembros, de oficio o atendiendo una solicitud concreta. Las peticiones entre Estados han de ser motivadas y siempre orientadas al cumplimiento de los fines previstos en esta ley orgánica.

Se contempla la posibilidad de que una autoridad competente española pueda dirigirse directamente a la Unidad de Información sobre Pasajeros de otro Estado miembro para una solicitud de información, siempre que se den conjuntamente las circunstancias de urgencia e imposibilidad de comunicación con la UIP nacional. En todo caso se remitirá copia de la petición a la UIP española.

La transferencia de datos a Europol se llevará a cabo electrónicamente y de forma motivada, siempre que entre dentro del ámbito de sus competencias y sea necesaria para el ejercicio de sus funciones.

Se incluye el procedimiento de transmisión de datos a terceros países. En este intercambio se tendrá que observar lo establecido en la legislación que transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención,

investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Además, deberá tratarse de una transmisión de datos necesaria para los fines de esta ley orgánica, y el Estado receptor de los mismos solamente podrá transmitirlos, a su vez, a otro tercer Estado si cuenta para ello con la expresa autorización de la Unidad española. En todo caso, se garantizará que la transmisión y la utilización de datos PNR a terceros Estados mantengan unos estándares y garantías como los previstos en esta ley orgánica.

En garantía del derecho a la intimidad de los sujetos afectados y en especial de su derecho a la protección de datos de carácter personal, se contempla que los datos PNR facilitados a la UIP por los sujetos obligados serán conservados durante cinco años a contar desde su transmisión. Una vez transcurridos seis meses desde su recepción, los datos PNR que permitan la identificación directa del pasajero serán despersonalizados mediante enmascaramiento, y solo se permitirá el acceso a la totalidad de los mismos previa aprobación por la autoridad judicial o por la persona titular de la Secretaría de Estado de Seguridad.

Cumplido el plazo de los cinco años serán suprimidos definitivamente, sin perjuicio de su utilización por parte de las autoridades competentes que los hayan recibido y que los estén utilizando en el marco de un asunto concreto a efectos de prevenir, detectar, investigar o enjuiciar delitos de terrorismo o delitos graves.

Por último, se regulan en este capítulo las competencias de la Agencia Española de Protección de Datos en su condición de autoridad nacional de control de datos PNR.

El capítulo III, que regula el régimen sancionador, se limita a establecer las especialidades estrictamente necesarias por razón de la materia, aplicándose en lo demás el régimen general previsto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Así, se definen los sujetos responsables, los regímenes especiales de responsabilidad y el concurso de normas; se tipifican las infracciones que se clasifican en muy graves, graves y leves; se determinan las sanciones según la infracción de que se trate, para cuya graduación se tendrá en cuenta la repercusión en la seguridad pública, la gravedad, o el beneficio obtenido, entre otras circunstancias; se determina la competencia sancionadora; y, finalmente, se incluyen las normas procedimentales especiales sobre los gastos derivados de la adopción de posibles medidas provisionales por parte del órgano competente para resolver, así como sobre la caducidad del procedimiento.

En las disposiciones adicionales se regula el plazo en el que las compañías aéreas deberán comunicar a la UIP el formato de datos y el protocolo de transmisión que utilizarán; se establece que las comunicaciones se harán según los procedimientos establecidos por la Secretaría de Estado de Seguridad; y se establecen normas referentes a la transmisión de los datos PNR remitidos a determinadas autoridades competentes como son el Centro Nacional de Inteligencia, las Direcciones Generales de la Policía y de la Guardia Civil, la Dirección Adjunta de Vigilancia Aduanera y los Jueces y Tribunales y el Ministerio Fiscal.

Además, contiene cuatro disposiciones finales, relativas al título competencial, a los preceptos que tienen carácter de ley orgánica, a la incorporación de derecho de la Unión Europea y a la entrada en vigor.

III

En la elaboración de esta ley orgánica se han observado los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, de acuerdo con el artículo 129 de la Ley 39/2015, de 1 de octubre. Se trata de una norma necesaria para la transposición de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, cuya aprobación goza de las garantías correspondientes al rango de ley orgánica por suponer un desarrollo de derechos fundamentales de los ciudadanos.

Por último, está incluida en el Plan Anual Normativo para 2018 aprobado por el Consejo de Ministros en su reunión de 7 de diciembre de 2017.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Esta ley orgánica, con el propósito de garantizar y proteger la vida y la seguridad de los ciudadanos, tiene por objeto regular:

a) La transferencia de datos del registro de nombres de los pasajeros (en adelante datos PNR), así como de la información de la tripulación referida en el artículo 5.3, correspondientes a vuelos internacionales y, en su caso, nacionales, en los términos y a los efectos previstos en el capítulo II.

b) El sistema de recogida, uso, almacenamiento, tratamiento, protección, acceso y conservación de los datos PNR, la transmisión de dichos datos a las autoridades competentes, así como el intercambio de los mismos con los Estados miembros de la Unión Europea, con Europol y con terceros países.

c) La determinación y atribución de las funciones de la Unidad de Información sobre Pasajeros española.

d) El régimen sancionador aplicable a las infracciones de conformidad con lo dispuesto en esta ley orgánica.

2. Los datos PNR podrán ser objeto de tratamiento únicamente con la finalidad de prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves que se enumeran en el artículo 4, y de acuerdo con los propósitos establecidos en el artículo 12.2.

Artículo 2. *Ámbito de aplicación.*

1. Esta ley orgánica será de aplicación, en todo caso, a los datos PNR correspondientes a las personas que viajen en los vuelos internacionales, tanto interiores como exteriores de la Unión Europea, con su salida del territorio español o llegada al mismo, o que hagan escala en él. En este último supuesto, siempre se entenderán comprendidos los pasajeros en tránsito o en conexión, con las precisiones establecidas en el apartado siguiente.

2. Su ámbito de aplicación se extiende a los vuelos comerciales y a los vuelos privados.

No será de aplicación a los vuelos realizados por aeronaves de Estado y por aeronaves privadas, fletadas por el Estado para la prestación o apoyo de servicios de interés militar y en general servicios estatales no comerciales, durante los vuelos dedicados exclusivamente a materializar tal prestación o apoyo, que se asimilarán a las aeronaves de Estado, a los trabajos aéreos, a la aviación general que no tenga por objeto el transporte de personas, a los servicios aeroportuarios, a los servicios de navegación aérea, a los vuelos relacionados con la producción de aeronaves civiles, a los vuelos de entrenamiento de tripulaciones, a los vuelos de traslado para mantenimiento y revisión y a los vuelos relacionados con funciones regulatorias.

3. Como medida extraordinaria y por el tiempo que resulte imprescindible, será de aplicación a las rutas o a los vuelos concretos nacionales, que no efectúen escalas en ningún otro Estado, siempre que existan indicios suficientes de una clara y contrastada situación de riesgo, con la finalidad de prevenir, detectar, investigar y enjuiciar los delitos a los que se refiere el artículo 4.

La determinación de tales rutas o vuelos será acordada por el Consejo de Ministros, a propuesta del titular del Ministerio del Interior, teniendo en cuenta el carácter extraordinario de la medida, su necesidad y proporcionalidad.

Artículo 3. *Sujetos obligados.*

1. Son sujetos obligados las compañías aéreas, entendiendo como tales las empresas de transporte aéreo con una licencia de explotación válida o similar para el transporte por vía aérea.

A los efectos de esta ley orgánica, la definición de empresa será la establecida en el Reglamento (CE) 1008/2008 del Parlamento Europeo y del Consejo, de 24 de septiembre de 2008, sobre normas comunes para la explotación de servicios aéreos en la Comunidad,

comprendiendo cualquier persona física o jurídica, con o sin fines de lucro, o cualquier organismo oficial dotado o no de personalidad jurídica propia.

En el caso de los vuelos privados serán sujetos obligados los operadores de las aeronaves bien sea como propietarios, arrendatarios o en virtud de otro título posesorio reconocido por la legislación vigente.

2. Son igualmente sujetos obligados las entidades de gestión de reserva de vuelos, entendiendo como tales a las entidades que gestionen reservas de vuelos de pasajeros y recaben datos PNR de los mismos, cualesquiera que sean los medios utilizados para ello, tales como los operadores turísticos o las agencias de viajes, que estarán obligadas en los términos previstos en el artículo 9.2.

Artículo 4. *Delitos de terrorismo y delitos graves.*

1. A los exclusivos efectos de esta ley orgánica, son delitos de terrorismo los contemplados en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, como delitos de las organizaciones y grupos terroristas y delitos de terrorismo.

2. Asimismo, a los exclusivos efectos de esta ley orgánica, son delitos graves aquellos que la ley castigue con una pena de prisión igual o superior a tres años por ser constitutivos de:

a) Pertenencia a una organización delictiva.
b) Trata de seres humanos.
c) Explotación sexual de niños y pornografía infantil.
d) Tráfico ilícito de estupefacientes y sustancias psicotrópicas.
e) Tráfico ilícito de armas, municiones y explosivos.
f) Corrupción.
g) Fraude, incluido el que afecte a los intereses financieros de la Unión Europea.
h) Blanqueo del producto del delito y falsificación de moneda, con inclusión del euro.
i) Delitos informáticos/ciberdelincuencia.
j) Delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas.
k) Ayuda a la entrada y residencia ilegales.
l) Homicidio voluntario, agresión con lesiones graves.
m) Tráfico ilícito de órganos y tejidos humanos.
n) Secuestro, detención ilegal y toma de rehenes.
ñ) Robo organizado y a mano armada.
o) Tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte.
p) Falsificación y violación de derechos de propiedad intelectual o industrial de mercancías.
q) Falsificación de documentos administrativos y tráfico de documentos administrativos falsos.
r) Tráfico ilícito de sustancias hormonales y otros factores de crecimiento.
s) Tráfico ilícito de materiales radiactivos o sustancias nucleares.
t) Violación.
u) Delitos incluidos en la jurisdicción de la Corte Penal Internacional.
v) Secuestro de aeronaves y buques.
w) Sabotaje.
x) Tráfico de vehículos robados.
y) Espionaje industrial.

Artículo 5. *Datos del Registro de Nombres de Pasajeros (datos PNR).*

1. Los datos PNR son el conjunto de datos relativos al viaje de un pasajero, reservado por él o en su nombre, que recoge la información necesaria para la gestión de la reserva.

2. Los datos PNR relativos a los pasajeros son los siguientes:

a) Localizador de registro PNR.
b) Fecha de reserva y de emisión del billete.
c) Fechas previstas del viaje.
d) Nombres y apellidos.

e) Dirección y datos de contacto (número de teléfono, dirección de correo electrónico).
f) Todos los datos de pago, incluida la dirección de facturación.
g) Itinerario completo del viaje para el PNR específico.
h) Información sobre viajeros frecuentes.
i) Agencia de viajes u operador de viajes.
j) Situación de vuelo del pasajero: confirmaciones, facturación, no comparecencia o pasajeros de última hora sin reserva.
k) Información PNR escindida o dividida.
l) Observaciones generales, incluida toda la información disponible sobre menores de dieciocho años no acompañados, como nombre, apellidos, y sexo del menor, edad, idiomas que habla, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de salida y vínculo con el menor, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de llegada y vínculo con el menor, agente en el lugar de salida y de llegada.
m) Información sobre el billete, incluidos el número del billete, la fecha de emisión, los billetes solo de ida y la indicación de la tarifa de los billetes electrónicos (Automatic Ticket Fare Quote).
n) Datos del asiento, incluido el número.
ñ) Información sobre códigos compartidos.
o) Toda la información relativa al equipaje.
p) Número de viajeros y otros nombres de viajeros que figuran en el PNR.
q) Cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema API), incluidos el tipo, número, país de emisión y fecha de expiración de cualquier documento de identidad, nacionalidad, apellidos, nombre, sexo, fecha de nacimiento, compañía aérea, número de vuelo, fecha de salida, fecha de llegada, aeropuerto de salida, aeropuerto de llegada, hora de salida y hora de llegada.
r) Todo el historial de cambios de los datos PNR indicados en los párrafos a) a q).

3. En el caso de los vuelos comerciales las disposiciones de esta ley orgánica serán aplicables, además de a los datos de los pasajeros, a los datos de la tripulación en el caso del párrafo q) y a los datos de cualquier otra persona a bordo señalados en los párrafos o) y q) del apartado anterior. Igualmente, en el caso de los vuelos privados, serán de aplicación a tales datos de los pasajeros y tripulantes.

CAPÍTULO II

Tratamiento de los datos PNR

Artículo 6. *Unidad de Información sobre Pasajeros.*

1. La Unidad de Información sobre Pasajeros española (UIP) se integra orgánicamente en el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior.
2. La UIP es la responsable del tratamiento de los datos PNR.

Artículo 7. *Funciones y facultades.*

1. La UIP realizará exclusivamente las siguientes funciones:

a) Recoger los datos PNR, almacenarlos, tratarlos y transferir, en su caso, dichos datos o el resultado de su tratamiento a las autoridades competentes.
b) Intercambiar tanto los datos PNR como el resultado de su tratamiento con las Unidades de Información sobre Pasajeros de otros Estados miembros de la Unión Europea, con Europol y con terceros países.

2. Para la realización de las funciones mencionadas en el apartado anterior, la UIP será responsable de:

a) Analizar, relacionar y valorar los datos obtenidos.
b) Establecer y actualizar criterios útiles para identificar a las personas que puedan estar implicadas en delitos de terrorismo y delitos graves, en cooperación, en su caso, con las autoridades competentes.

c) Elaborar informes de inteligencia estratégica y de análisis de riesgo.

d) Colaborar con las autoridades competentes encargadas de las investigaciones y actuaciones operativas, así como elaborar los protocolos de actuación pertinentes en colaboración con las mismas.

e) Poner los hechos que puedan ser constitutivos de las infracciones previstas en esta ley orgánica en conocimiento del órgano competente para sancionarlas.

f) Elaborar estadísticas anuales sobre su actividad, incluyendo el número total de personas cuyos datos PNR hayan sido recopilados e intercambiados, así como el número de personas identificadas para un examen ulterior.

3. El almacenamiento, tratamiento y análisis de los datos PNR se llevará a cabo exclusivamente en uno o varios lugares seguros dentro del territorio nacional.

4. Cuando fuere preciso para el desarrollo de sus funciones, el personal al servicio de las autoridades competentes enumeradas en el artículo 14 podrá prestar servicios en la UIP. Dicho personal continuará en servicio activo en su Cuerpo dependiendo orgánica, funcional y retributivamente de su Administración de origen, sin perjuicio de que en el desarrollo de sus funciones en la UIP haya de atenerse a lo preceptuado para la misma respecto a su organización y funcionamiento.

Artículo 8. *Responsable de protección de datos.*

1. La UIP designará una persona como responsable de protección de los datos PNR que velará por que se adopten las medidas oportunas para controlar el tratamiento de estos datos y por que se apliquen las garantías en materia de protección de datos. El responsable de protección de datos actuará como punto de contacto único, al que cualquier interesado tendrá derecho a dirigirse para todas las cuestiones relativas al tratamiento de sus datos PNR.

2. La persona designada lo será atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos personales, y a su capacidad para desempeñar las funciones contempladas en esta ley orgánica. Deberá contar con los medios necesarios para el desempeño de sus funciones de manera eficaz e independiente.

3. La persona responsable de la protección de datos tendrá acceso a todos los datos PNR tratados por la UIP. Si considerase que el tratamiento de un dato no ha sido lícito, lo pondrá en conocimiento del responsable del tratamiento para que se adopten las medidas correctoras necesarias y, si lo estima oportuno, podrá remitir el asunto a la autoridad nacional de control.

4. En lo no previsto en esta ley orgánica se regirá por lo regulado para los delegados de protección de datos en la legislación que transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, y hasta ese momento por las normas que regulen en Derecho español el tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

Artículo 9. *Obligaciones de transmisión de datos.*

1. Las compañías aéreas enviarán los datos PNR correspondientes a los vuelos comprendidos en el artículo 2 que hayan recopilado en el transcurso normal de su actividad, a la base de datos de la UIP. En el caso de los vuelos privados, el operador asumirá la responsabilidad de que la información prevista en el artículo 5.3 sea remitida a la UIP.

En el caso de que existan varias compañías aéreas relacionadas con un mismo vuelo, la obligación de transmitir los datos recaerá en la compañía aérea que actúe como operadora del mismo.

2. Las entidades de gestión de reservas de vuelos introducirán en el PNR los datos que hayan recopilado en el transcurso normal de su actividad respecto a los vuelos comprendidos en el artículo 2.

3. En el cumplimiento de sus obligaciones de información, y sin perjuicio de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y en la legislación interna que se dicte en uso de la habilitación contenida en aquel, los sujetos obligados informarán a las personas a las que se refieran los datos PNR del motivo de su recogida y de su destinatario, la Unidad de Información sobre Pasajeros, ante cuyo responsable de protección de datos podrán dirigirse para todas las cuestiones relativas al tratamiento de sus datos PNR.

4. Las compañías aéreas enviarán los datos PNR a la UIP, utilizando en todo caso medios electrónicos que ofrezcan garantías suficientes en relación con las medidas de seguridad técnicas y las medidas organizativas que rigen el tratamiento de datos que se va a llevar a cabo. Esta transmisión se realizará con arreglo a uno de los formatos de datos y mediante uno de los protocolos de transmisión establecidos en la Decisión de Ejecución de la Comisión (UE) 2017/759, de 28 de abril de 2017, relativa a los protocolos comunes y los formatos de datos que deberán utilizar las compañías aéreas para la transmisión de los datos PNR a las Unidades de Información sobre Pasajeros.

En el caso de que transmitan datos API sobre los pasajeros de manera separada respecto del resto de los datos PNR para el mismo vuelo, deberán utilizar, para su envío a la UIP, el formato específico de datos que contempla la Decisión de Ejecución de la Comisión (UE) 2017/759, de 28 de abril de 2017.

En caso de fallo técnico o imposibilidad sobrevenida, realizarán la transmisión de los datos PNR, en el plazo más breve posible, por cualquier otro medio apropiado que garantice un nivel adecuado de seguridad de dichos datos.

5. Las compañías aéreas que no operen vuelos con arreglo a un calendario concreto y público y que no dispongan de la infraestructura técnica necesaria para usar los formatos de datos y los protocolos de transmisión incluidos en la Decisión de Ejecución de la Comisión (UE) 2017/759, de 28 de abril de 2017, utilizarán, para la transmisión de los datos PNR, los formatos y los medios electrónicos que se acuerden de forma bilateral entre la compañía aérea y el Ministerio del Interior, siempre que ofrezcan garantías suficientes respecto de las medidas de seguridad técnicas. Este régimen será el aplicable en todo caso a los vuelos privados.

Artículo 10. *Momentos de la transmisión de datos.*

1. Los momentos en los que las compañías aéreas deben transmitir los datos PNR a la UIP serán los siguientes:

a) Entre las 24 y las 48 horas antes de la hora de salida programada del vuelo, e

b) inmediatamente después del cierre del vuelo, una vez que los pasajeros hayan embarcado en el avión en preparación de la salida y no sea posible embarcar o desembarcar.

Las compañías aéreas podrán limitar esta transmisión prevista en el párrafo b) a las actualizaciones de la información transmitida conforme al párrafo a).

2. El Proveedor de Servicios de Navegación Aérea en el espacio aéreo de soberanía española, comunicará a la UIP los cambios de destino, así como las escalas no programadas que le sean notificados por la tripulación de la aeronave o por otro Proveedor de Servicios de Navegación Aérea».

3. Además, cuando sea necesario acceder a los datos PNR para responder a una amenaza real y concreta relacionada con delitos de terrorismo o con delitos graves, en momentos distintos de los previstos en el apartado 1, todos los sujetos obligados, caso por caso, deberán transmitir a la UIP dichos datos con carácter inmediato al requerimiento recibido.

Artículo 11. *Régimen jurídico aplicable al tratamiento de datos PNR.*

1. Los tratamientos de datos de carácter personal que lleven a cabo la UIP y las autoridades competentes referidas en el artículo 14 se regirán por esta ley orgánica y supletoriamente por la legislación que transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y hasta ese momento por las normas que regulen en Derecho español el tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales. En este régimen jurídico se incluye la protección de los datos personales de los pasajeros y sus derechos de acceso, rectificación, supresión, limitación del tratamiento, indemnización y recurso judicial.

2. Sin perjuicio de las obligaciones establecidas en esta ley orgánica, los tratamientos de datos de carácter personal realizados por los sujetos obligados referidos en el artículo 3 se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y por la legislación interna que se dicte en uso de la habilitación contenida en aquel.

Artículo 12. *Tratamiento de los datos PNR.*

1. Los datos PNR serán recogidos por la UIP.

Si la información transmitida incluyera datos distintos de los relacionados en esta ley orgánica, la UIP los suprimirá inmediatamente y de manera definitiva en el momento de su recepción.

2. La UIP tratará los datos PNR solo para los siguientes propósitos:

a) Realizar una evaluación de los pasajeros y de la tripulación antes de la llegada o salida programada del vuelo, a fin de identificar a las personas que deban ser examinadas de nuevo por las autoridades competentes y, en su caso, por Europol ante la posibilidad de que pudieran estar implicadas en un delito de terrorismo o en un delito grave.

b) Responder en cada caso particular a las peticiones de las autoridades competentes, debidamente motivadas y con suficiente base, para que les transfieran datos PNR en supuestos específicos a efectos de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, así como el resultado de su tratamiento.

c) Analizar los datos PNR con el fin de establecer o actualizar criterios que deben utilizarse en las evaluaciones realizadas en virtud del apartado 3.b), con el objeto de identificar a las personas que puedan estar implicadas en delitos de terrorismo o delitos graves.

Estos criterios de evaluación predeterminados deberán ser proporcionados y específicos y estar orientados a la finalidad que persiguen. No se basarán en el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato o partido político, la salud o la vida u orientación sexual de la persona. La UIP establecerá y revisará periódicamente estos criterios, en colaboración con las autoridades competentes.

3. Al realizar la evaluación a que se refiere el apartado 2.a), la UIP podrá someter los datos PNR a las siguientes operaciones:

a) Comparará los datos PNR con todas las bases de datos disponibles y pertinentes, a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.

b) Tratará los datos PNR de acuerdo con los criterios predeterminados establecidos para identificar a las personas que puedan estar implicadas en delitos de terrorismo o en delitos graves.

4. Cuando la evaluación efectuada de acuerdo con el apartado 2.a) arrojara un resultado positivo, la UIP procederá a la revisión individual de tal resultado a través de medios no automatizados, con el fin de comprobar la necesidad de que las autoridades competentes realicen un examen ulterior o emprendan las acciones o inicien los procedimientos oportunos. A tal fin, la UIP deberá transmitir los datos PNR a las autoridades competentes.

Artículo 13. *Consecuencias de la evaluación.*

Las consecuencias de las evaluaciones de los pasajeros a las que se refiere el apartado 2.a) del artículo anterior, no perjudicarán el derecho de entrada en España de las personas que gocen del derecho de libre circulación en la Unión Europea.

Cuando estas evaluaciones se efectúen en relación con pasajeros de vuelos interiores de la Unión Europea a los que sea aplicable el Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras, las consecuencias se ajustarán a lo previsto en dicho reglamento.

Artículo 14. *Autoridades competentes.*

1. Las autoridades competentes para solicitar o recibir de la UIP datos PNR o el resultado del tratamiento de dichos datos a fin de seguir examinando esa información o de adoptar las medidas adecuadas para prevenir, detectar, investigar y enjuiciar delitos de terrorismo y delitos graves, serán las siguientes:

a) La Dirección General de la Policía.
b) La Dirección General de la Guardia Civil.
c) El Centro Nacional de Inteligencia.
d) La Dirección Adjunta de Vigilancia Aduanera.
e) El Ministerio Fiscal.
f) Las correspondientes de las Comunidades Autónomas que hayan asumido estatutariamente competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana, y cuenten con un cuerpo de policía propio.

2. Las peticiones de datos realizadas por las autoridades competentes serán debidamente motivadas y con suficiente base. En ningún caso se admitirán peticiones masivas y no fundamentadas.

3. Las autoridades competentes colaborarán con la UIP, en el ámbito de sus competencias, para el cumplimiento de los fines de esta ley orgánica.

4. A los Jueces y Tribunales, que tendrán la consideración de autoridades competentes, no les serán de aplicación los apartados 2 y 3, en atención al principio constitucional de independencia del poder judicial, rigiéndose en cuanto a las peticiones de datos y a la colaboración con la UIP por lo que establezca la legislación aplicable al ejercicio de la función jurisdiccional.

5. Los datos remitidos por la UIP a las autoridades competentes podrán ser objeto de tratamiento posterior por estas, únicamente con los fines específicos de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, sin perjuicio de las acciones o procedimientos que puedan realizarse o iniciarse en el caso de que, como consecuencia del tratamiento de dichos datos, se detecten otros delitos o indicios de ellos.

6. Las autoridades competentes no adoptarán ninguna decisión que produzca efectos jurídicos adversos para una persona o que afecte negativamente a una persona únicamente en razón del tratamiento automatizado de datos PNR.

Dichas decisiones no deberán basarse en el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato o partido político, la salud o la vida y orientación sexual de la persona.

Artículo 15. *Protección de los datos de carácter personal.*

1. La UIP no podrá tratar datos PNR que revelen el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato o partido político, la salud, la vida o la orientación sexual de la persona. En el caso de que reciba datos PNR que revelen tal información, los suprimirá inmediatamente.

2. La UIP conservará la documentación relativa a todos los sistemas y procedimientos de tratamiento bajo su responsabilidad.

Dicha documentación constará como mínimo de los siguientes elementos:

a) Los datos identificativos del personal de la UIP encargado del tratamiento de los datos PNR, así como del responsable de protección de datos, y los distintos niveles de autorización de acceso;

b) las solicitudes cursadas por las autoridades competentes y por las Unidades de Información sobre Pasajeros de otros Estados miembros y;

c) todas las solicitudes y transmisiones de datos PNR a un tercer país o a Europol.

La UIP pondrá esta documentación a disposición de la autoridad nacional de control a petición de esta, de acuerdo con la legislación vigente.

3. La UIP llevará registros, al menos, de las operaciones de recogida, consulta, transferencia y supresión de los datos.

Los registros de consulta y transferencia mostrarán, en particular, la finalidad, la fecha y la hora de tales operaciones y, en la medida de lo posible, la identidad de la persona que consultó o transmitió los datos PNR y la identidad de los receptores de dichos datos.

Los registros se utilizarán exclusivamente a efectos de verificación, autocontrol, y garantía de la integridad de los datos y de su seguridad o de auditoría. Dichos registros se conservarán por un período de cinco años.

La UIP pondrá los registros a disposición de la autoridad nacional de control a petición de esta, de acuerdo con la legislación aplicable.

4. Cuando sea probable que una violación de los datos personales dé lugar a un elevado riesgo para la protección de estos o afecte negativamente a la intimidad del interesado, la UIP comunicará, sin demora injustificada, dicha violación al interesado y a la autoridad nacional de control.

5. La UIP aplicará las medidas y los procedimientos técnicos y organizativos adecuados para garantizar un elevado nivel de seguridad correspondiente a los riesgos que entrañen el tratamiento y las características de los datos PNR.

Artículo 16. *Intercambio de información entre Estados miembros de la Unión Europea.*

1. La UIP transmitirá los datos PNR pertinentes y necesarios o el resultado de su tratamiento, relativos a las personas identificadas por la misma como personas que puedan estar implicadas en un delito de terrorismo o en un delito grave, a las Unidades de Información sobre Pasajeros de los otros Estados miembros. Dicha transmisión sólo se llevará a cabo tras un análisis de cada caso y, en supuestos de tratamiento automatizado de los datos PNR, tras una revisión individualizada por medios no automatizados.

En caso de que la UIP reciba datos PNR o el resultado de su tratamiento de la Unidad de Información sobre Pasajeros de otro Estado miembro deberá proporcionar todos los datos pertinentes y necesarios, a las autoridades competentes correspondientes, tras una revisión individualizada.

2. La UIP tendrá derecho a solicitar, en cada caso concreto, para la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo o delitos graves, a la Unidad de Información sobre Pasajeros de cualquier otro Estado miembro, que le suministre los datos PNR almacenados en su base de datos y que no hayan sido despersonalizados mediante enmascaramiento de elementos de los datos, así como, si fuera necesario, el resultado de cualquier tratamiento de los mismos. La solicitud deberá ser debidamente motivada.

En el caso de que hayan sido despersonalizados mediante enmascaramiento de elementos de datos, la transmisión tendrá lugar de conformidad con el derecho nacional aplicable en el Estado miembro de la Unidad de Información sobre Pasajeros requerida.

3. A su vez, la Unidad de Información sobre Pasajeros de cualquier Estado miembro podrá solicitar directamente a la UIP datos PNR o el resultado de su tratamiento, bajo las mismas condiciones previstas en el apartado anterior. En ese caso, la UIP proporcionará la información solicitada lo antes posible.

En el supuesto de que los datos requeridos hayan sido despersonalizados mediante enmascaramiento, la UIP únicamente proporcionará los datos completos o el resultado de su tratamiento ante casos específicos cuando sea necesario para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, y sólo cuando lo

haya autorizado la autoridad judicial o la persona titular de la Secretaría de Estado de Seguridad.

4. Las autoridades competentes que requieran datos PNR recabados por un Estado miembro de la Unión Europea canalizarán sus solicitudes de forma motivada a través de la UIP.

Únicamente cuando no sea posible dirigir sus peticiones a través de la UIP y en caso de urgencia, y siempre que la solicitud cumpla con las condiciones establecidas en el apartado 2, las autoridades competentes podrán solicitar dichos datos directamente a la Unidad de Información sobre Pasajeros de otro Estado miembro.

De estas solicitudes directas y urgentes se remitirá copia a la UIP, al mismo tiempo que a la Unidad de Información sobre Pasajeros del Estado miembro de que se trate, que deberá acompañarse, lo antes posible, de una motivación de la remisión directa.

5. De manera excepcional, cuando sea necesario acceder a los datos PNR para responder a una amenaza concreta y real relacionada con delitos de terrorismo o delitos graves, la UIP solicitará a la Unidad de Información sobre Pasajeros del Estado miembro correspondiente que acceda a los datos PNR fuera de los momentos ordinarios de transmisión establecidos en el artículo 10 y que se los transmita.

Del mismo modo, la UIP responderá lo antes posible a las solicitudes que reciba de otros Estados miembros en los supuestos previstos en el párrafo anterior.

6. El intercambio de información previsto en este artículo podrá realizarse utilizando cualquiera de las vías existentes de cooperación entre las autoridades competentes de los Estados miembros.

Artículo 17. *Transferencia de datos a Europol.*

1. La UIP transferirá los datos PNR específicos o el resultado de su tratamiento solicitados por Europol, caso por caso, de forma electrónica y debidamente motivada, cuando sea estrictamente necesario para apoyar y reforzar la acción de un Estado miembro de la Unión Europea a efectos de prevenir, detectar, investigar o enjuiciar delitos de terrorismo o delitos graves, siempre que el delito entre dentro del ámbito de competencias de Europol y para el desempeño de sus funciones.

2. La solicitud indicará las causas razonables por las que Europol considera que la transmisión de los datos PNR o de los resultados de su tratamiento va a contribuir significativamente a prevenir, detectar o investigar la infracción penal en cuestión.

3. Europol informará al responsable de la protección de datos de cada uno de los intercambios de información en virtud de este artículo.

4. El intercambio de información se realizará a través de la Red de Intercambio Seguro de Información (SIENA).

Artículo 18. *Transferencias de datos a terceros países no miembros de la Unión Europea.*

1. La UIP podrá transferir a terceros países no miembros de la UE datos PNR, así como el resultado de su tratamiento, en casos concretos y si se cumplen concurrentemente los siguientes requisitos:

a) Las condiciones establecidas para las transferencias de datos a terceros países en la legislación que transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y hasta ese momento por las normas que regulen en Derecho español el tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

b) La transmisión resulta necesaria para los fines señalados en el artículo 1.2.

c) El tercer país se compromete a transmitir los datos PNR a otro tercer país sólo si fuera estrictamente necesario para los fines de esta ley orgánica y siempre contando con la autorización expresa de la UIP.

d) Los previstos en el artículo 16.

2. Las transmisiones de datos PNR por la UIP sin consentimiento previo del Estado miembro del que fueron obtenidos se permitirán en circunstancias excepcionales y únicamente si:

a) Son esenciales para responder a una amenaza específica y real relacionada con delitos de terrorismo o delitos graves de un Estado miembro o de un tercer país y;

b) el consentimiento previo no pudo obtenerse a su debido tiempo.

La UIP informará sin demora a la autoridad del Estado miembro responsable de dar el consentimiento. La transmisión se registrará por la UIP y podrá ser objeto de una verificación posterior.

3. Cada vez que la UIP transfiera datos PNR a terceros países en virtud de lo previsto en este artículo, su responsable de protección de datos será informado.

4. La UIP exclusivamente transmitirá datos PNR a las autoridades competentes de terceros países tras asegurarse de que se ajustan a un estándar de condiciones y garantías equivalente al de esta ley orgánica y de que la utilización de los datos PNR prevista por los receptores se ajusta a dichas condiciones y garantías.

Artículo 19. *Período de conservación de los datos y despersonalización.*

1. Los datos PNR proporcionados a la UIP por los sujetos obligados se conservarán en una base de datos de la Unidad durante un plazo de cinco años a partir de la fecha de su transmisión a la UIP.

2. Transcurrido un plazo de seis meses desde la transmisión a la que se refiere el apartado 1, todos los datos PNR deberán ser despersonalizados mediante enmascaramiento, de manera que resulten invisibles para un usuario los siguientes elementos que servirían para identificar directamente a los afectados:

a) Nombres y apellidos, incluidos los de otros pasajeros que figuran en el PNR, y número de personas que figuran en el PNR que viajan juntas;

b) dirección y datos de contacto;

c) todos los datos sobre el pago, incluida la dirección de facturación, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el registro PNR, o a cualquier otra persona;

d) información sobre viajeros frecuentes;

e) observaciones generales, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el registro, y

f) todos los datos API sobre los pasajeros.

3. Al finalizar el período de seis meses mencionado en el apartado 2, solo se permitirá la transmisión de los datos completos cuando concurran las dos circunstancias siguientes:

a) Que sea necesario a los efectos establecidos en el artículo 12.2.b).

b) Que haya sido aprobada por una autoridad judicial o por la persona titular de la Secretaría de Estado de Seguridad. En este último caso, se informará de la transmisión al responsable de protección de datos de la UIP, y estará sujeta a la revisión, *a posteriori*, por parte del mismo.

4. Los datos PNR serán suprimidos de modo permanente al finalizar el período a que se refiere el apartado 1. Esta obligación se entenderá sin perjuicio de aquellos casos en que se hayan transferido datos PNR específicos a una autoridad competente y esta los esté utilizando en el marco de un asunto concreto a efectos de prevenir, detectar, investigar o enjuiciar delitos de terrorismo o delitos graves, en cuyo caso la conservación de los datos por la autoridad competente se regirá por la normativa específica.

5. Los resultados del tratamiento a que se refiere el artículo 12.2.a) serán conservados por la UIP durante el tiempo necesario para informar de un resultado positivo a las autoridades competentes y a las Unidades de Información sobre Pasajeros de otros Estados miembros.

Cuando el resultado de un tratamiento automatizado, tras un examen individual por medios no automatizados, arroje un resultado negativo, se podrá almacenar para evitar falsos resultados positivos posteriores, mientras los datos de base no se hayan eliminado según el apartado 4.

Artículo 20. *Competencias de la Agencia Española de Protección de Datos.*

Además de las competencias que le otorga su normativa específica, la Agencia Española de Protección de Datos, en su condición de autoridad nacional de control de datos PNR a los efectos previstos en esta ley orgánica, ejercerá las siguientes competencias:

a) Asesorar, previa solicitud, sobre la aplicación de las disposiciones adoptadas en España para aplicar la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y controlar su aplicación con el fin de proteger los derechos fundamentales de cualquier interesado en lo relativo al tratamiento de datos personales.

b) Conocer de las reclamaciones presentadas contra los tratamientos realizados al amparo de esta ley orgánica y dar respuesta a las mismas en un plazo de tiempo razonable.

c) Verificar la legalidad de los tratamientos, por propia iniciativa o como consecuencia de una reclamación, para lo cual podrá realizar investigaciones, inspecciones y auditorías, de acuerdo con lo dispuesto en su normativa reguladora, sin perjuicio de las funciones que corresponden al Consejo General del Poder Judicial como autoridad de control de los tratamientos de datos vinculados al ejercicio de la función jurisdiccional.

CAPÍTULO III

Régimen sancionador

Sección 1.ª Disposiciones generales

Artículo 21. *Sujetos responsables.*

La responsabilidad por las infracciones cometidas recaerá directamente en los sujetos obligados que, por acción u omisión, realizaran la conducta en que consista la infracción.

Artículo 22. *Responsable de tratamiento y responsable de protección de datos.*

La responsabilidad del responsable de tratamiento de los datos PNR y del responsable de protección de datos PNR se determinará de acuerdo con lo dispuesto en la legislación que transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y hasta ese momento por las normas que regulen en Derecho español el tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

Artículo 23. *Regla especial.*

A los efectos exclusivos de esta ley orgánica, se entenderá que los incumplimientos de la obligación de transmisión o remisión de los datos PNR que se produzcan en relación a un mismo vuelo constituyen una única infracción.

Artículo 24. *Concurso de normas.*

1. Siempre que no constituyan infracciones a la normativa general de protección de datos de carácter personal, los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de esta u otra ley orgánica se sancionarán observando las siguientes reglas:

a) El precepto especial se aplicará con preferencia al general.

b) El precepto más amplio o complejo absorberá el que sancione las infracciones subsumidas en aquel.

c) En defecto de los criterios anteriores, se aplicará el precepto que sancione los hechos con la sanción mayor.

2. En el caso de que un solo hecho constituya dos o más infracciones, o cuando una de ellas sea medio necesario para cometer la otra, la conducta será sancionada por aquella infracción a la que se aplique una mayor sanción.

Sección 2.ª Infracciones

Artículo 25. *Clasificación de las infracciones.*

Las infracciones tipificadas en esta ley orgánica se clasifican en muy graves, graves y leves.

Artículo 26. *Infracciones muy graves.*

Constituyen infracciones muy graves:

a) La falta de remisión de los datos PNR, de acuerdo con lo establecido en el artículo 10.1 y 2, cuando se haya generado un riesgo grave para la seguridad ciudadana, la vida o la integridad física de las personas.

b) La falta de remisión de los datos PNR, conforme a los formatos y protocolos a los que se refiere el artículo 9.4, cuando se haya generado un riesgo grave para la seguridad ciudadana, la vida o la integridad física de las personas.

c) En caso de requerimiento previo, la falta de remisión de los datos PNR o la remisión fuera del plazo concedido al efecto, cuando se haya generado un riesgo grave para la seguridad ciudadana, la vida o la integridad física de las personas.

d) La falta de transmisión de los datos PNR a la UIP en los supuestos a los que se refiere el artículo 10.3.

Artículo 27. *Infracciones graves.*

Constituyen infracciones graves:

a) La falta de remisión de los datos PNR, de acuerdo con lo establecido en el artículo 10.1 y 2.

b) La falta de remisión de los datos PNR, conforme a los formatos y protocolos a los que se refiere el artículo 9.4.

c) La falta de adopción en tiempo y forma, por parte de los sujetos obligados, de las medidas necesarias para realizar legalmente las transmisiones.

d) En caso de requerimiento previo, la falta de remisión de los datos PNR o la remisión fuera del plazo establecido al efecto o sin cumplir con los requisitos técnicos y legales de transmisión.

e) Las omisiones en la transmisión de datos.

f) La falta de comunicación, conforme a lo dispuesto en esta ley orgánica, de cualquier cambio producido previamente o durante el trayecto, respecto al destino donde se tuviera previsto aterrizar.

g) La falta de diligencia en el mantenimiento de los sistemas electrónicos seguros de transmisión de los datos PNR siempre que no constituya infracción con arreglo a la normativa general de protección de datos de carácter personal.

Artículo 28. *Infracciones leves.*

Constituyen infracciones leves:

a) El incumplimiento de la obligación de informar a la UIP sobre los formatos de datos y protocolos de transmisión en el plazo previsto.

b) Cualquier otro incumplimiento de lo previsto en esta ley orgánica y que no constituya infracción grave o muy grave.

Sección 3.ª Sanciones

Artículo 29. *Sanciones.*

Las infracciones muy graves serán sancionadas con multa de 60.001 a 300.000 euros; de 20.001 a 60.000 euros las graves; y de 3.000 a 20.000 euros las leves.

Artículo 30. *Graduación de las sanciones.*

Atendiendo al principio de proporcionalidad, se graduará la cuantía de las sanciones teniendo en cuenta, entre otras, las siguientes circunstancias, además de las previstas en el artículo 29 de la Ley 40/2015, de 1 de octubre:

a) La incidencia en la seguridad pública y/o en los derechos a la intimidad, la protección de datos, la imagen o el honor de las personas.
b) El beneficio económico obtenido como consecuencia de la comisión de la infracción.
c) La naturaleza, gravedad y duración de la infracción, teniendo en cuenta el número de afectados y los daños o perjuicios que hayan sufrido.
d) El grado de cooperación para poner remedio o mitigar los posibles efectos adversos.

Artículo 31. *Competencia sancionadora.*

Son órganos competentes para la imposición de las sanciones:

a) La persona titular del Ministerio del Interior, para la sanción de las infracciones muy graves.
b) La persona titular de la Secretaría de Estado de Seguridad, para la sanción de las infracciones graves y leves.

Sección 4.ª Normas especiales de procedimiento sancionador

Artículo 32. *Medidas provisionales.*

Los gastos ocasionados por la adopción de las posibles medidas provisionales serán de cuenta del causante de los hechos objeto del procedimiento sancionador. Dichos gastos, en su caso, serán reclamables mediante el procedimiento administrativo de apremio cuando la sanción adquiera firmeza en vía administrativa.

Artículo 33. *Caducidad del procedimiento.*

El procedimiento caducará transcurrido un año desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concurra identidad de sujeto, hecho y fundamento, hasta la finalización de este.

Artículo 34. *Acceso a los datos de otras Administraciones públicas.*

Los órganos competentes para imponer las sanciones previstas en esta ley orgánica podrán acceder, en el ejercicio de dichas competencias, a los datos relativos a los sujetos infractores que estén directamente relacionados con la investigación de los hechos constitutivos de infracción, con las debidas garantías de seguridad, integridad y disponibilidad. El acceso y el tratamiento posterior de los datos se realizarán, en todo caso, de conformidad con lo establecido en la normativa reguladora de protección de datos de carácter personal.

Disposición adicional primera. *Plazo para comunicar los formatos de datos y protocolos de transmisión.*

Las compañías aéreas informarán a la UIP del formato de datos y del protocolo de transmisión que utilizarán, en el plazo de cuarenta días a contar desde la fecha de publicación en el «Boletín Oficial del Estado» de esta ley orgánica. El formato y el protocolo deberán estar entre los previstos en la Decisión de Ejecución (UE) 2017/759 de la Comisión, de 28 de abril de 2017.

Disposición adicional segunda. *Transmisión de datos PNR.*

Las transmisiones de datos PNR se realizarán según los medios de transmisión establecidos por la Secretaría de Estado de Seguridad, de acuerdo con lo dispuesto en el artículo 9.

Disposición adicional tercera. *Régimen jurídico del acceso por el Centro Nacional de Inteligencia a datos PNR.*

El acceso a los datos PNR por parte del Centro Nacional de Inteligencia y su control, se realizarán de acuerdo con lo previsto en esta ley orgánica, salvaguardando, en todo caso, el carácter de materia legalmente clasificada como secreto de sus actividades y objetivos, con el fin de dar cumplimiento a las misiones y funciones establecidas en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

Disposición adicional cuarta. *Transmisiones de datos PNR a las Direcciones Generales de la Policía y de la Guardia Civil y a las autoridades competentes de las Comunidades Autónomas que cuenten con un cuerpo de policía propio e integral.*

Las transmisiones de datos PNR a las Direcciones Generales de la Policía y de la Guardia Civil y su control, se realizarán de acuerdo con lo previsto en esta ley orgánica, salvaguardando, en todo caso, el carácter reservado de sus investigaciones y de la inteligencia generada en torno a dichos datos en relación a delitos de terrorismo y demás delitos graves.

Igual régimen de transmisión y salvaguarda de sus investigaciones e inteligencia que las contempladas en el párrafo anterior se aplicarán a las autoridades competentes de las Comunidades Autónomas que hayan asumido competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana y cuenten con cuerpo de policía propio.

Disposición adicional quinta. *Transmisiones de datos PNR a la Dirección Adjunta de Vigilancia Aduanera.*

Las transmisiones de datos PNR a la Dirección Adjunta de Vigilancia Aduanera y su control, se harán de acuerdo con lo previsto en esta ley orgánica, salvaguardando, en todo caso, el carácter reservado de los datos con trascendencia tributaria, de acuerdo con la Ley 58/2003, de 17 de diciembre, General Tributaria, de sus investigaciones y de la inteligencia generada en torno a dichos datos en relación a delitos graves de su competencia.

Disposición adicional sexta. *Transmisiones de datos PNR a Jueces, Tribunales y Ministerio Fiscal.*

Las transmisiones de datos PNR a Jueces, Tribunales y Ministerio Fiscal se harán de acuerdo con lo previsto en esta ley orgánica, sin perjuicio de la aplicación a su tratamiento de la legislación reguladora del ejercicio de la potestad jurisdiccional.

En particular, las transmisiones de datos PNR a Jueces y Tribunales se efectuarán de acuerdo con lo previsto en el artículo 14.4 de esta ley orgánica.

Disposición final primera. *Título competencial.*

Esta ley orgánica se dicta al amparo de lo previsto en el artículo 149.1.1.ª y 29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales, y sobre la seguridad pública, respectivamente.

Disposición final segunda. *Preceptos que tienen carácter de ley orgánica.*

1. Tienen carácter orgánico los siguientes preceptos:

a) Los artículos 4 y 5.
b) El capítulo II.
c) La disposición final segunda.

2. Los preceptos no incluidos en el apartado anterior tienen carácter de ley ordinaria.

Disposición final tercera. *Incorporación de derecho de la Unión Europea.*

Mediante esta ley orgánica se incorpora al Derecho español la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

Disposición final cuarta. *Entrada en vigor.*

Esta ley orgánica entrará en vigor a los dos meses de su publicación en el «Boletín Oficial del Estado», excepto la disposición adicional primera, que entrará en vigor al día siguiente de dicha publicación.

§ 77

Real Decreto 957/2020, de 3 de noviembre, por el que se regulan los estudios observacionales con medicamentos de uso humano. [Inclusión parcial]

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 310, de 26 de noviembre de 2020
Última modificación: sin modificaciones
Referencia: BOE-A-2020-14960

[. . .]

CAPÍTULO II

Condiciones para la realización de los estudios observacionales con medicamentos

[. . .]

Artículo 5. *Consentimiento informado y protección de los datos personales de los sujetos participantes.*

1. Los estudios observacionales con medicamentos que conlleven entrevistar al sujeto participante, requerirán su consentimiento informado.

No obstante, siguiendo las disposiciones aplicables de la normativa vigente y los principios éticos para las investigaciones médicas en seres humanos, se podrá eximir de solicitar el consentimiento informado, siempre que el CEIm considere que la investigación observacional tiene un valor social importante, que su realización no sería factible o viable sin dicha dispensa, y que entraña riesgos mínimos para los participantes.

2. Para la solicitud del consentimiento informado se tendrán en cuenta, en su caso, las normas y principios éticos relativos a las previsiones en relación con la recogida, almacenamiento y posible uso futuro de las muestras biológicas de los sujetos.

3. Los promotores de los estudios que utilicen alguna fuente de información que incluya el tratamiento de datos personales deberán tener en cuenta lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, en particular, lo siguiente:

a) El promotor deberá haber evaluado y mitigado, mediante las medidas apropiadas en cada caso, el impacto que la realización del estudio puede tener en la protección de datos personales.

b) El promotor y los investigadores del estudio deben garantizar la confidencialidad de los datos de los sujetos participantes.

c) Sin perjuicio de lo dispuesto en el apartado 1, será necesario el consentimiento del sujeto participante a no ser que sea de aplicación otra base legítima para el tratamiento de sus datos personales de entre las referidas en los artículos 6.1 y 9.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Además, el promotor y los investigadores deberán aplicar los criterios que rigen el tratamiento de datos en la investigación en salud de conformidad con la disposición adicional decimoséptima de la Ley Orgánica 3/2018, de 5 de diciembre.

d) Las condiciones de acceso a los datos personales deberán detallarse en el protocolo, incluyendo las condiciones de su transmisión internacional fuera del ámbito del Espacio Económico Europeo, si ello está previsto.

4. Cuando se trate de un estudio con datos anónimos o que hayan sido sometidos a un tratamiento de seudonimización, el protocolo recogerá el procedimiento seguido para conseguir dicha anonimización o seudonimización.

5. El acceso a los datos de los sujetos participantes se realizará, en todo caso, en las condiciones que establezca el responsable del tratamiento de dichos datos, de modo que se garantice el cumplimento de la normativa sobre protección de datos personales.

[. . .]

§ 78

Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 239, de 5 de octubre de 1979
Última modificación: 5 de junio de 2021
Referencia: BOE-A-1979-23708

[. . .]

TÍTULO II

Del régimen penitenciario

CAPÍTULO I

Organización general

[. . .]

Artículo quince bis. *Tratamientos de datos de carácter personal.*

1. Admitido en el establecimiento un interno, se procederá a verificar su identidad personal, efectuando la reseña alfabética, dactilar y fotográfica, así como a la inscripción en el libro de ingresos y a la apertura de un expediente personal relativo a su situación procesal y penitenciaria, respecto del que se reconoce el derecho de acceso. Este derecho sólo se verá limitado de forma individualizada y fundamentada en concretas razones de seguridad o tratamiento.

2. El tratamiento de los datos personales de los internos se regirá por lo previsto en la Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Los datos personales de categorías especiales que no figuren en el apartado anterior se podrán tratar con el consentimiento del interesado. Sólo se prescindirá de dicho consentimiento cuando sea estrictamente necesario y se efectúe con las garantías adecuadas para proteger el derecho a la protección de datos de los interesados, atendiendo al tipo de datos que se traten y a las finalidades de los distintos tratamientos dirigidos a la ejecución de la pena.

3. Igualmente se procederá al cacheo de su persona y al registro de sus efectos, retirándose los enseres y objetos no autorizados.

4. En el momento del ingreso se adoptarán las medidas de higiene personal necesarias, entregándose al interno las prendas de vestir adecuadas que precise, firmando el mismo su recepción.

[. . .]

§ 79

Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 134, de 5 de junio de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-9347

[. . .]

CAPÍTULO XII

De la Agencia Española de Protección de Datos

Artículo 52. *De la Agencia Española de Protección de Datos.*

1. La Agencia Española de Protección de Datos ejercerá las funciones y potestades que le corresponden de acuerdo con lo previsto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal, con el fin de garantizar una protección específica de los datos personales de las personas menores de edad en los casos de violencia ejercida sobre la infancia y la adolescencia, especialmente cuando se realice a través de las tecnologías de la información y la comunicación.

2. La Agencia garantizará la disponibilidad de un canal accesible y seguro de denuncia de la existencia de contenidos ilícitos en Internet que comportaran un menoscabo grave del derecho a la protección de datos personales.

3. Se permitirá a las personas menores de edad, que así lo soliciten, formular denuncia por sí mismas y sin necesidad de estar acompañadas de una persona adulta, siempre que el funcionario público encargado estime que tiene madurez suficiente.

4. Las personas mayores de catorce años podrán ser sancionadas por hechos constitutivos de infracción administrativa de acuerdo con la normativa sobre protección de datos personales.

5. Cuando la autoría de los hechos cometidos corresponda a una persona menor de dieciocho años, responderán solidariamente con ella de la multa impuesta sus progenitores, tutores, acogedores y guardadores legales o de hecho, por este orden, en razón al incumplimiento del deber de cuidado y vigilancia para prevenir la infracción administrativa que se impute a las personas menores de edad.

[. . .]

§ 80

Ley 10/2021, de 9 de julio, de trabajo a distancia. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 164, de 10 de julio de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-11472

[. . .]

CAPÍTULO III

Derechos de las personas trabajadoras a distancia

[. . .]

Sección 5.ª Derechos relacionados con el uso de medios digitales

Artículo 17. *Derecho a la intimidad y a la protección de datos.*

1. La utilización de los medios telemáticos y el control de la prestación laboral mediante dispositivos automáticos garantizará adecuadamente el derecho a la intimidad y a la protección de datos, en los términos previstos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, de acuerdo con los principios de idoneidad, necesidad y proporcionalidad de los medios utilizados.

2. La empresa no podrá exigir la instalación de programas o aplicaciones en dispositivos propiedad de la persona trabajadora, ni la utilización de estos dispositivos en el desarrollo del trabajo a distancia.

3. Las empresas deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos legal y constitucionalmente. En su elaboración deberá participar la representación legal de las personas trabajadoras.

Los convenios o acuerdos colectivos podrán especificar los términos dentro de los cuales las personas trabajadoras pueden hacer uso por motivos personales de los equipos informáticos puestos a su disposición por parte de la empresa para el desarrollo del trabajo a distancia, teniendo en cuenta los usos sociales de dichos medios y las particularidades del trabajo a distancia.

[. . .]

CAPÍTULO IV

Facultades de organización, dirección y control empresarial en el trabajo a distancia

Artículo 20. *Protección de datos y seguridad de la información.*

1. Las personas trabajadoras, en el desarrollo del trabajo a distancia, deberán cumplir las instrucciones que haya establecido la empresa en el marco de la legislación sobre protección de datos, previa participación de la representación legal de las personas trabajadoras.

2. Las personas trabajadoras deberán cumplir las instrucciones sobre seguridad de la información específicamente fijadas por la empresa, previa información a su representación legal, en el ámbito del trabajo a distancia.

Artículo 21. *Condiciones e instrucciones de uso y conservación de equipos o útiles informáticos.*

Las personas trabajadoras deberán cumplir las condiciones e instrucciones de uso y conservación establecidas en la empresa en relación con los equipos o útiles informáticos, dentro de los términos que, en su caso, se establezcan en la negociación colectiva.

Artículo 22. *Facultades de control empresarial.*

La empresa podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por la persona trabajadora de sus obligaciones y deberes laborales, incluida la utilización de medios telemáticos, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, sus circunstancias personales, como la concurrencia de una discapacidad.

[. . .]

Información relacionada

- Téngase en cuenta que la presente Ley proviene de la tramitación como proyecto de ley del Real Decreto-Ley 28/2020, de 22 de septiembre. Ref. BOE-A-2020-11043

§ 81

Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 312, de 29 de diciembre de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-21650

TÍTULO PRELIMINAR

Disposiciones generales

[. . .]

CAPÍTULO II

Organización administrativa para la lucha contra el dopaje

[. . .]

Artículo 6. *Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte.*

1. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte es el organismo público adscrito al Ministerio con competencias en la política deportiva, de los previstos en el artículo 84.1.a).3.º de la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, a través del cual se elaboran y ejecutan las políticas de lucha contra el dopaje, correspondiéndole la planificación, la realización de controles y la tramitación y resolución de los expedientes sancionadores.

2. La organización, funciones y procedimientos de actuación de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte se determinarán en sus estatutos de conformidad con lo previsto en esta ley, aplicándose supletoriamente la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas. En todo caso, contará con un Comité Sancionador Antidopaje, con la naturaleza, composición y funciones previstas en el capítulo III del título II de esta ley, y un Comité de Autorizaciones de Uso Terapéutico, que ejercerá las competencias establecidas en el artículo 17.

En su órgano colegiado de gobierno participarán los agentes del deporte y, dentro de los mismos, específicamente, las federaciones deportivas.

La Agencia contará con un órgano de participación, coordinación y seguimiento en el que estarán representados los y las deportistas, así como los órganos y organismos competentes en materia de lucha contra el dopaje de las Comunidades Autónomas.

3. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte actúa con plena independencia funcional cuando establece y ejecuta medidas de control del dopaje sobre los y las deportistas sujetos a la presente ley, no pudiendo recibir órdenes o

instrucciones de órgano o autoridad algunos en el ejercicio de sus funciones y, especialmente, en la instrucción y resolución de los procedimientos sancionadores cuya competencia le esté atribuida.

4. Para la realización de las funciones que le atribuya su estatuto, la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte podrá formalizar convenios o conciertos con cualesquiera entidades públicas o privadas, de conformidad con lo establecido en la Ley 40/2015, de 1 de octubre, y en su caso, en la legislación de contratos del sector público.

5. En su condición de organismo especializado en la investigación, control y ejecución de la política contra el dopaje en el deporte, la comisión se configura como el organismo público estatal de asesoramiento y colaboración con las Fuerzas y Cuerpos de Seguridad del Estado, la policía judicial y los demás poderes públicos con competencias relacionadas con su ámbito de actuación y, a requerimiento de éstos, con los jueces y tribunales.

6. Los miembros de los órganos mencionados en el presente artículo y de los demás que puedan integrarse en el seno de la comisión se designarán conforme a criterios de profesionalidad y amplio reconocimiento en el mundo del deporte y de la lucha contra el dopaje, así como de acuerdo con el principio de presencia equilibrada de mujeres y hombres, salvo razones objetivamente fundadas y debidamente motivadas. Se entenderá por presencia equilibrada el 50 % de mujeres y 50 % de hombres.

7. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte se rige por lo dispuesto en la presente ley, en la sección 4.ª del capítulo III, del título II, de la Ley 40/2015, de 1 de octubre, y en el resto de las normas que le sean de aplicación.

[. . .]

TÍTULO I

Controles de dopaje

[. . .]

Artículo 14. *Garantías en la práctica de los controles. Personal habilitado para su realización.*

1. Los controles de dopaje siempre se realizarán por el personal expresamente habilitado por la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte para el desempeño de esta función.

2. El otorgamiento de la habilitación requerirá el cumplimiento de los requisitos de capacidad, titulación y formación que se establezcan mediante Orden de la persona titular del Ministerio de Cultura y Deporte, de acuerdo con lo previsto en la normativa aplicable.

En todo caso, la habilitación para la realización de controles que consistan en la extracción de sangre del deportista sólo podrá otorgarse a personal sanitario con capacitación legal para realizar dicha extracción.

3. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte y los órganos competentes de las Comunidades Autónomas podrán desarrollar un sistema de reconocimiento mutuo de habilitaciones mediante la suscripción de convenios específicos.

4. Asimismo, podrá realizar las funciones de control de dopaje el personal que se encuentre habilitado por las federaciones internacionales, por la Agencia Mundial Antidopaje o por las organizaciones nacionales antidopaje de otros países. Los controles de dopaje así realizados o cualquiera de las actuaciones en ellos comprendida serán plenamente validos a los efectos previstos en esta ley.

5. Los funcionarios de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte y el personal expresamente habilitado por ésta para la realización de los controles de dopaje tendrán, en sus actos de servicio o con motivo de los mismos, la consideración de agentes de la autoridad, a los efectos en su caso, de la exigencia de la responsabilidad que proceda a quienes se resistan u obstaculicen su labor de control.

En el ejercicio de las funciones señaladas en el apartado primero del presente artículo, el citado personal podrá requerir a las personas a las que se refiere el apartado 2 del artículo 3 cuantas informaciones fueran necesarias a efectos del control de dopaje o de la

investigación de cualesquiera infracciones tipificadas en esta ley y, en su caso, denunciarán ante el órgano competente para la incoación del correspondiente expediente sancionador, las conductas y actuaciones que contravengan las disposiciones establecidas en la misma y en sus normas de desarrollo.

Asimismo, podrán solicitar, a través de la autoridad gubernativa correspondiente, el apoyo necesario de los cuerpos y fuerzas de seguridad.

6. Los hechos constatados directamente por el personal referido en el apartado anterior tendrán valor probatorio cuando se formalicen en documento público, observando los requisitos legales pertinentes, sin perjuicio de las pruebas que en defensa de sus respectivos derechos o intereses puedan señalar o aportar los propios interesados.

Artículo 15. *Condiciones de realización de los controles.*

1. Para facilitar el descanso nocturno del deportista, dentro de la franja horaria comprendida entre las 23:00 y las 06:00 horas no se procederá a la realización de controles de dopaje fuera de competición, salvo que el deportista, en cumplimiento de la obligación prevista en el artículo 10.3 de esta ley fijare su localización en un horario comprendido en aquella franja horaria.

No obstante, en casos debidamente justificados, y de acuerdo con el principio de proporcionalidad, será posible su realización siempre que en el momento de llevarlo a cabo se informe al deportista de las razones que justifican la no observancia de la limitación horaria establecida en el párrafo anterior.

2. Los controles de dopaje se realizarán con pleno respeto a los derechos fundamentales de la persona y a la protección de su intimidad y datos personales.

Asimismo, se ajustarán al principio de mínima intervención, con observancia del principio de proporcionalidad.

3. Los y las deportistas serán informados en el momento de recibir la notificación del control y, en su caso, al iniciarse la recogida de la muestra, de los derechos y obligaciones que les asisten en relación con el citado control, de los trámites esenciales del procedimiento y de sus principales consecuencias, del tratamiento y cesión de los datos previstos en la presente ley, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, supresión y oposición, establecidos en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4. A los efectos de los procedimientos disciplinarios en materia de dopaje, la negativa sin justificación válida a someterse a los controles, una vez documentada, constituirá prueba suficiente a los efectos de exigir la responsabilidad disciplinaria del deportista.

No serán justificaciones válidas para negarse al control de dopaje las circunstancias de tiempo o lugar o de cualquier otra naturaleza que hayan sido buscadas o decididas intencionadamente por el deportista.

Se considera justificación válida la imposibilidad de acudir al control de dopaje como consecuencia acreditada de lesión que impida objetivamente someterse al mismo, o cuando la realización del control ponga en grave riesgo la salud del deportista.

El documento que acredite la negativa sin justificación válida a que se refiere el párrafo anterior, realizada por el personal habilitado, será suficiente para iniciar el correspondiente procedimiento disciplinario, sin perjuicio del derecho de defensa del interesado.

5. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte establecerá un modelo normalizado de información para la recogida de las muestras en la realización de los controles de dopaje.

Artículo 16. *Competencia y registro de tratamientos médicos.*

1. Las federaciones, clubes, organizaciones, grupos y demás entidades deportivas a las que se refiere el título III de la Ley 10/1990, de 15 de octubre, del Deporte, o que participen en actividades o competiciones deportivas organizadas en el marco de la citada ley, podrán exigir la llevanza de un libro de registro que deberá estar debidamente registrado en la entidad que lo acordara, y de cuya integridad exista garantía, en el que harán constar las

autorizaciones de uso terapéutico y los tratamientos médicos y sanitarios que hayan prescrito sus facultativos a los y las deportistas bajo su dirección, siempre que estos autoricen dicha inscripción; y extendiendo una copia o certificación de cada asiento, a instancia de los y las deportistas, donde conste identificado el facultativo o profesional sanitario que, bajo su dirección, hubiera prescrito o realizado el tratamiento médico o sanitario, con expresión de la fecha y la firma o el sello del profesional sanitario.

Las entidades a que se refiere el párrafo anterior podrán complementar o sustituir el libro registro por procedimientos centralizados de base de datos con utilización de las tecnologías de la información y la comunicación e identificación electrónica, como la firma digital y los sistemas de historia electrónica única y centralizada.

2. Por su parte, las federaciones podrán desarrollar internamente, un reglamento para formalizar y establecer las obligaciones de los clubes que participen en sus competiciones nacionales con respecto al registro de los tratamientos médicos y sanitarios de los y las deportistas.

3. Dichos libros y certificaciones tendrán la consideración de documento sanitario a los efectos de acceso a la información que contiene y de custodia y protección de datos, y estará sometido a la legislación vigente en materia de derechos y obligaciones de información y documentación clínica, receta médica y órdenes de dispensación, y al resto de la legislación general sobre salud pública y acceso a la información pública.

4. No obstante, el contenido de estos libros podrá ser requerido por el órgano competente para resolver los expedientes sancionadores por dopaje, o aportado a instancia de parte como medio de prueba en los procedimientos sancionadores, a los efectos de determinar la concurrencia de criterios eximentes o atenuantes de la responsabilidad por las infracciones previstas en esta ley.

[. . .]

TÍTULO II

Régimen sancionador en materia de dopaje

[. . .]

CAPÍTULO II

Del procedimiento para la imposición de sanciones

[. . .]

Artículo 36. *Información y diligencias reservadas.*

1. Corresponde a la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte, en el ámbito de sus competencias, la realización de las investigaciones y averiguaciones necesarias para asegurar el cumplimiento de lo previsto en esta ley y, en particular, la práctica de diligencias reservadas previamente al inicio de un procedimiento sancionador.

2. Las actuaciones y diligencias previas se orientarán a determinar, con la mayor precisión posible, los hechos susceptibles de motivar la incoación del procedimiento, la identificación de la persona o personas que pudieran resultar responsables y las circunstancias relevantes que concurran en unos y otros.

3. Las actuaciones y diligencias previas serán realizadas por los órganos y personal de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte que tengan atribuidas funciones de investigación, averiguación e inspección en la materia, y, en defecto de éstos, por la persona u órgano administrativo que determine el órgano competente para la iniciación del procedimiento sancionador.

4. Las diligencias reservadas darán lugar a la iniciación del procedimiento sancionador cuando quede acreditada la existencia de indicios de la infracción, procediéndose, en otro caso, al archivo de las mismas.

5. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte iniciará diligencias reservadas para investigar al personal de apoyo de los y las deportistas en los

casos en que le conste la existencia de una infracción cometida con un menor o persona protegida, o cuando algún miembro del personal de apoyo de los y las deportistas haya trabajado o colaborado con más de un deportista sancionado por una infracción en materia de dopaje.

6. Toda autoridad o funcionario público que tenga constancia de la posible existencia de una infracción administrativa en materia de dopaje deberá ponerlo sin dilación en conocimiento de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte.

[. . .]

TÍTULO III

Tratamiento de datos personales relativos al dopaje

Artículo 50. *Responsabilidad del personal que presta servicios para la realización de los controles.*

1. El personal que desempeñe las funciones de control del dopaje deberá guardar confidencialidad y secreto respecto de los asuntos que conozca por razón de las funciones que desarrolla.

2. Los datos personales, obtenidos en el desarrollo de sus funciones, incluidos los que se deriven del análisis las muestras cedidas conforme a lo previsto en el artículo 18 de esta ley, solo podrán utilizarse para los fines para los cuales han sido recogidos y, en su caso, para la denuncia de hechos que puedan ser constitutivos de infracción administrativa o de delito. También podrán ser utilizados para estudios científicos, siempre que no se revele la identidad de las personas.

3. Sin perjuicio de la responsabilidad que proceda, de acuerdo con la legislación específicamente aplicable, en particular en materia de protección de datos de carácter personal, las infracciones en la custodia y, en su caso, la divulgación, comunicación y cesión ilegítima de los datos personales relativos a los controles y procedimientos en materia de dopaje tienen la consideración de infracción muy grave respecto de aquel personal que ostente la condición de empleado público de acuerdo con lo previsto en el artículo 95.2.p) del texto refundido de la Ley del Estatuto Básico del Empleado Público aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y su legislación de desarrollo.

[. . .]

Artículo 52. *Autorización de cesión de datos personales.*

Los datos relativos a los controles de dopaje podrán ser cedidos, en los términos previstos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales, en consonancia con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, a los organismos internacionales públicos o privados de los que España sea parte y que participen en la lucha contra el dopaje en el ámbito deportivo, en el marco de lo que dispongan los compromisos internacionales legalmente vinculantes asumidos por España, o para realizar estadísticas o estudios de investigación.

La cesión de datos relativos a controles de dopaje con fines estadísticos o de investigación científica solo podrá hacerse cuando tal cesión sea proporcional al objetivo perseguido, respete en lo esencial el derecho a la protección de datos y se protejan suficientemente los intereses y derechos fundamentales del interesado.

TÍTULO IV

Control y supervisión general de los productos susceptibles de producir dopaje en el deporte

CAPÍTULO I

Medidas de control y supervisión de productos, medicamentos y complementos nutricionales

[. . .]

Artículo 55. *Potestad de inspección.*

1. Corresponde a la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte en el ámbito de sus competencias la realización de las inspecciones necesarias para asegurar el cumplimiento de lo previsto en esta ley.

La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte velará por el cumplimiento de esta ley, realizando las inspecciones oportunas, con funcionarios con la debida cualificación y formación universitaria en las materias pertinentes.

La potestad de inspección de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte se desarrollará en los términos y con los límites y condiciones establecidos en la presente ley y sin perjuicio de la necesidad de recabar, en su caso, la autorización o ratificación judicial prevista en el apartado sexto del artículo 8 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

2. Las actuaciones de inspección que lleve a cabo la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte se realizarán por funcionarios públicos que, en el ejercicio de sus funciones, tendrán la condición de agentes de la autoridad y, por tanto, la consideración de autoridad pública.

Los inspectores de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte serán provistos de un documento oficial que acredite su condición, que será expedido por el Director de la misma.

Los inspectores de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte en su ejercicio gozarán de plena autonomía técnica y funcional, y se les garantizará protección frente a todo tipo de violencia, coacción y amenaza, e independencia frente a cualquier influencia indebida.

Los inspectores de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte que desarrollen las funciones de inspección, cuando ejerzan tales funciones y acrediten su identidad, estarán autorizados para:

a) Entrar libremente y sin previa notificación, en cualquier momento, en todo establecimiento o instalación deportiva, centro deportivo, servicio deportivo, entidad deportiva o evento deportivo que pueda estar sujeto a esta ley.

b) Proceder a las pruebas, investigaciones o exámenes necesarios para comprobar el cumplimiento de esta ley y de las normas que se dicten para su desarrollo.

c) Tomar muestras de productos o muestras biológicas, en orden a la comprobación del cumplimiento de lo previsto en esta ley y en las disposiciones para su desarrollo. En todo caso, la toma de muestras biológicas deberá sujetarse a lo dispuesto en esta ley para la protección de datos en la toma de muestras en los controles de dopaje.

d) Incautar los medicamentos y productos sanitarios que no hayan sido notificados tal y como se prevé en el artículo 53.

e) Realizar cuantas actuaciones sean precisas en orden al cumplimiento de las funciones de inspección que desarrollen.

Las actas levantadas por los inspectores de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte tendrán el carácter de documento público y, salvo que se acredite lo contrario, harán prueba de los hechos que en ellas se recojan.

3. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte, en el desempeño de sus funciones, podrá solicitar la colaboración de las Fuerzas y Cuerpos de Seguridad.

En los casos en los que el Director lo considere oportuno, los funcionarios debidamente acreditados de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte podrán auxiliarse de expertos, técnicos y especialistas que resulten de especial interés en las tareas de inspección. Los mismos no tendrán la consideración de agentes de la autoridad y su actividad únicamente se circunscribirá al auxilio y colaboración con el personal inspector, a las órdenes de los cuales ejercerán su labor.

4. Específicamente, la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte, podrá inspeccionar los botiquines deportivos, locales y otros elementos que permitan custodiar o albergar los productos y sustancias susceptibles de dar un resultado analítico adverso en un control de dopaje. Las personas o entidades que tengan acceso a estos botiquines deportivos, locales y otros elementos, deberán permitir, en todo momento, el acceso a sus locales y archivos a la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte para realizar dichas inspecciones.

Del mismo modo, las Fuerzas y Cuerpos de Seguridad del Estado, los servicios de inspección sanitaria del Estado así como los órganos de las Comunidades Autónomas que tengan atribuida competencia para ello, por su propia iniciativa o a instancia de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte, podrán inspeccionar los botiquines deportivos, locales y otros elementos que permitan custodiar o albergar los productos y sustancias susceptibles de dar un resultado analítico adverso en un control de dopaje, sin perjuicio de lo dispuesto en el apartado sexto del artículo 8 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en los casos en que sea aplicable.

5. A los efectos del ejercicio de la potestad sancionadora por la Administración, se tendrá en cuenta el tipo de sustancias, el número de unidades, la justificación terapéutica, así como el resto de cuestiones directamente vinculadas a su ejercicio profesional.

6. Mediante orden de la persona titular del Ministerio de Cultura y Deporte, se establecerá el contenido admisible de los botiquines y, específicamente, de aquellos medicamentos y productos sanitarios que resultan necesarios para atender las contingencias derivadas de cualquier urgencia médica.

La custodia, conservación y dispensación de estos medicamentos deberá cumplir con lo establecido en la normativa específica vigente que le sea de aplicación.

7. De los resultados de los controles aduaneros sobre botiquines y demás instrumentos previstos en el apartado 4 de este artículo que realicen la Agencia Estatal de Administración Tributaria y los órganos competentes para el control sanitario en frontera en el desarrollo de sus funciones se informará al órgano competente en los términos que se establezcan mediante Orden de la persona titular del Ministerio de Cultura y Deporte.

8. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte, de oficio o a requerimiento de las autoridades aduaneras, podrá inspeccionar dichos botiquines, en orden a la comprobación del cumplimiento de lo previsto en esta ley y en las disposiciones para su desarrollo, en relación con los productos y sustancias susceptibles de dar un resultado analítico adverso en un control de dopaje. Ambos tipos de actuaciones se realizarán aplicando lo previsto en el artículo 42 del Reglamento (UE) n.º 952/2013 del Parlamento Europeo y del Consejo, de 9 de octubre de 2013, por el que se establece el código aduanero de la Unión.

[. . .]

Disposición adicional cuarta. *Protección de datos de carácter personal.*

1. Los tratamientos de datos personales regulados en la presente ley se llevarán a cabo conforme a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Los derechos de acceso, rectificación y supresión se ejercitarán conforme a la normativa referida en el párrafo anterior.

2. Son datos de carácter personal objeto de su tratamiento para la consecución de las finalidades de interés público previstas en esta ley todos aquellos que resulten imprescindibles para el desarrollo y ejecución de las actuaciones, técnicas y procedimientos que se articulan en garantía del desarrollo de las competiciones deportivas limpias, en condiciones de igualdad y de protección de la salud de los y las deportistas. En particular son objeto de tratamiento datos identificativos de los y las deportistas, de salud, de localización de deportistas, de infracciones y sanciones administrativas y en su caso penales, entre otros.

3. Las finalidades perseguidas con el tratamiento de los datos recabados en virtud de las disposiciones de la presente ley son la prevención y persecución del dopaje en el deporte, así como también garantizar el desarrollo de las competiciones deportivas en términos de igualdad y de acuerdo con las capacidades naturales y preparación de los y las deportistas. También lo será el tratamiento de los datos recabados con fines estadísticos o para la realización de estudios de investigación científica.

4. Son responsable del tratamiento la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte, las Comunidades Autónomas de acuerdo con sus respectivos ámbitos competenciales y de acuerdo con los Convenios suscritos entre estos y aquella que resulten de aplicación.

5. Serán encargados del tratamiento de datos todas aquellas empresas, entidades, organizaciones o profesionales autónomos que, para prestar servicios a la Agencia Española de un servicio a un tercero (otra empresa, entidad, organización o profesional autónomo), accedan y traten necesariamente datos de carácter personal de los que la Agencia Española Comisión Española para la Lucha Antidopaje sea Responsable de Tratamiento.

Los encargados del tratamiento realizarán su cometido de acuerdo con las instrucciones del responsable del tratamiento en virtud de lo establecido en artículo 28 del Reglamento (UE) 2016/679. En particular los procesos de realización de controles de dopaje serán realizados respetando las garantías establecidas en la legislación vigente.

6. Son destinatarios de los datos el Consejo Superior de Deportes, los laboratorios de control de dopaje, organizaciones nacionales e internacionales antidopaje, las federaciones deportivas nacionales e internacionales, los organizadores de competiciones deportivas, ligas profesionales o clubes o sociedades deportivas que tengan interés legítimo, órganos de resolución de conflictos cualquiera que sea su ámbito territorial, los órganos jurisdiccionales, el Ministerio Fiscal y las Fuerzas y Cuerpos de Seguridad.

Los destinatarios serán también responsables del tratamiento de los datos que hubiera sido objeto de comunicación conforme a las disposiciones de la presente ley y a la normativa que les resulte de aplicación por el mismo tratamiento.

7. La base jurídica principal del tratamiento de acuerdo con el objetivo y finalidad de la presente ley es el cumplimiento de un interés público esencial, así como el ejercicio de poderes públicos en el cumplimiento de una misión realizada en interés público de acuerdo con lo dispuesto en los artículos 9.2.g), 6.1.e), y 89 del Reglamento (UE) 2016/679.

Además existen tratamientos cuya base jurídica se encuentra en la letra c) del artículo 6.1 del Reglamento (UE) 2016/679 en relación con el cumplimiento de una obligación legal aplicable al responsable del tratamiento, así como el consentimiento del interesado del apartado a) del mismo artículo para uno o varios fines específicos.

En cuanto al tratamiento de categorías especiales de datos será de aplicación lo previsto en el artículo 9.2.g) del Reglamento (UE) 2016/679 y en su caso la prevista en la letra i) del mismo apartado y concordantes de los previstos en el artículo 6 del Reglamento (UE) 2016/679.

La base jurídica aplicable a las transferencias de datos personales a terceros países u organizaciones internacionales y de acuerdo con la declaración contenida en el considerando 112 del Reglamento (UE) 2016/679 que alude expresamente como excepción a la prohibición de trasferencias la eliminación del dopaje en el deporte, será el artículo 49.1.d) del Reglamento (UE) 2016/679.

8. Los datos recogidos se limitarán a los necesarios para el cumplimiento de las finalidades descritas, de acuerdo con el principio de minimización de datos.

9. La recolección de datos se hará conforme a la legislación vigente con especial atención al cumplimiento del deber de información previa a los interesados sobre las condiciones, derechos y obligaciones del tratamiento, así como a los posibles destinatarios en los términos previstos en la ley.

Los datos objeto de tratamiento podrán ser también comunicados a los órganos jurisdiccionales, al Ministerio Fiscal o a las Fuerzas y Cuerpos de Seguridad para el ejercicio de sus competencias de investigación de delitos o faltas de acuerdo con lo previsto en esta ley orgánica, sin perjuicio de la aplicación a su tratamiento de la legislación reguladora del ejercicio de la potestad jurisdiccional o las que en su caso resultaren de aplicación.

La comunicación de los datos de carácter personal de los interesados en los procesos de control de dopaje se realiza según la normativa de protección de datos aplicable y la establecida en la presente ley y en su normativa de desarrollo.

Las muestras obtenidas de los controles de dopaje no irán acompañadas de información personal de los sujetos objeto del control, sino que serán categorizadas con un código numérico que evite la identificación de los interesados.

10. De acuerdo con la finalidad del tratamiento, se conservarán los datos recogidos en virtud de las disposiciones legales durante el tiempo necesario para el cumplimiento del fin para el cual fueron recogidos y en su caso por el tiempo necesario para atender a las responsabilidades derivadas de su tratamiento ante los órganos administrativos o jurisdiccionales competentes. Una vez trascurrido dicho periodo de conservación, los datos serán suprimidos de manera que se imposibilite la correlación o identificación de los mismos con los interesados.

11. Las administraciones públicas que sean responsables del tratamiento deberán garantizar la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta, en todo caso, lo prevenido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Los demás responsables del tratamiento deberán garantizar la aplicación de las medidas de seguridad análogas a las anteriores, garantizándose el empleo de la tecnología adecuada para el tratamiento de datos, de acuerdo con el estado de la técnica y de las necesidades y procurándose, en las comunicaciones que contengan información personal, el uso del cifrado o encriptado.

12. El ejercicio de derechos para las personas físicas sujetas a la normativa de protección de datos se garantizará conforme a dicha normativa. Serán atendidas las solicitudes de tales derechos por el responsable del tratamiento en los términos establecidos en la legislación vigente.

[. . .]

ANEXO

Definiciones

1. Actividades antidopaje: Educación e información para la lucha contra el dopaje, planificación de la distribución de los controles, mantenimiento de un grupo registrado de control, gestión de los pasaportes biológicos de los y las deportistas, realización de controles, organización de análisis de muestras, recopilación de información y realización de investigaciones, tramitación de solicitudes de AUT, gestión de resultados, audiencias, seguimiento y exigencia del cumplimiento de las sanciones impuestas y todas las demás actividades de lucha contra el dopaje según lo previsto en el Código y/o las Normas Internacionales.

2. Administración: La provisión, suministro, supervisión, facilitación u otra participación en el uso o tentativa de uso por otra persona de una sustancia prohibida o método prohibido. No obstante, esta definición no incluirá las acciones de personal médico de buena fe que supongan el uso de una sustancia prohibida o método prohibido con fines terapéuticos genuinos y legales o con otra justificación aceptable, y tampoco las acciones que impliquen el uso de sustancias prohibidas que no estén prohibidas en los controles fuera de competición, salvo que las circunstancias, tomadas en su conjunto, demuestren que dichas

sustancias prohibidas no están destinadas a fines terapéuticos genuinos y legales o tienen por objeto mejorar el rendimiento deportivo.

3. Agencia Mundial Antidopaje (AMA): Fundación creada y regida por el Derecho Suizo para combatir el dopaje en el deporte.

4. Anulación: Ver Consecuencias de la infracción de las normas antidopaje.

5. Audiencia preliminar: Vista de las alegaciones formuladas por el interesado, por escrito o de modo oral, en el plazo improrrogable de cinco días siguientes a la recepción de la notificación de una suspensión provisional.

6. Autorización de Uso Terapéutico (AUT): Autorización por medio de la cual un deportista sometido a un tratamiento médico, queda facultado para hacer uso de una sustancia prohibida o un método prohibido contenido en la Lista de Sustancias y Métodos Prohibidos, concedida por el Comité de Autorizaciones de Uso Terapéutico de acuerdo con el procedimiento establecido.

7. Ausencia de culpa o de negligencia: Demostración por parte de un deportista u otra persona de que ignoraba, no sospechaba y no podía haber sabido o presupuesto razonablemente, incluso aplicando la mayor diligencia, que había usado o se le había administrado una sustancia prohibida o un método prohibido o que había infringido de algún otro modo una norma antidopaje. Excepto en el caso de una persona protegida o un deportista aficionado, para cualquier infracción prevista en el artículo 20.a), el deportista deberá demostrar también cómo se introdujo la sustancia prohibida en su organismo.

8. Ausencia de culpa o de negligencia graves: Demostración por parte del deportista u otra persona de que, dado el conjunto de circunstancias y teniendo en cuenta los criterios de ausencia de culpa o de negligencia, no existió negligencia o su culpa no fue significativa respecto de la infracción de la norma antidopaje. Excepto en el caso de una persona protegida o un deportista aficionado, para cualquier infracción prevista en el artículo 20.a), el deportista deberá demostrar también cómo se introdujo en su organismo la sustancia prohibida.

9. Ayuda sustancial: A los efectos de lo dispuesto en los artículos 26.3.d) y 34.1 de esta ley, una persona que proporcione ayuda sustancial deberá: (1) revelar por completo mediante una declaración escrita y firmada toda la información que posea en relación con las infracciones de las normas antidopaje, y (2) colaborar plenamente en la investigación y las decisiones que se tomen sobre cualquier caso relacionado con esa información, lo que incluye, por ejemplo, testificar ante cualquier organismo jurisdiccional o durante una audiencia si así se le exige por parte de una organización antidopaje o tribunal de expertos. Asimismo, la información facilitada debe ser creíble y constituir una parte importante del caso abierto o, en caso de no haberse iniciado éste, debe haber proporcionado un fundamento suficiente sobre el cual podría haberse tramitado un caso.

10. Código: El Código Mundial Antidopaje y las definiciones que se contienen en el anexo del mismo para su interpretación.

11. Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte (CELAD): Organización Nacional Antidopaje de España. Es el organismo público a través del cual se realizan las políticas estatales de lucha contra el dopaje.

12. Comité Olímpico Nacional: La organización reconocida como tal por el Comité Olímpico Internacional.

13. Comité Sancionador Antidopaje: Órgano competente para resolver los expedientes sancionadores por infracciones de dopaje previstos en esta ley, de acuerdo con el artículo 47.

14. Competición: Una prueba única, un partido, una partida o un concurso deportivo concreto.

15. Consecuencias de la infracción de las normas antidopaje («Consecuencias»): La infracción por parte de un deportista o de otra persona de una norma antidopaje puede suponer alguna o varias de las consecuencias siguientes:

a) Anulación significa la invalidación de los resultados de un deportista en una competición o acontecimiento concreto, con todas las consecuencias resultantes, como la retirada de las medallas, los puntos y los premios;

b) Suspensión significa que se prohíbe al deportista o a otra persona durante un periodo de tiempo determinado o a perpetuidad, participar, en calidad alguna, en ninguna

competición o actividad en los términos del artículo 30.1 y 30.4 y obtener financiación en los términos del artículo 30.5;

c) Suspensión provisional significa que se prohíbe temporalmente al deportista u otra persona participar en cualquier Competición o actividad hasta que se dicte la decisión definitiva en el procedimiento sancionador regulado en el capítulo II del título II;

d) Consecuencias económicas significa una sanción económica impuesta por una infracción de las normas antidopaje o con el objeto de resarcirse de los costes asociados a dicha infracción; y

e) Divulgación o información pública significa la difusión o distribución de información al público general o a personas no incluidas en el personal autorizado a tener notificaciones previas de acuerdo con los artículos 37, 38, 41 y 43 de esta ley. En los deportes de equipo, los equipos también podrán ser objeto de las consecuencias previstas en el artículo 22 de la presente ley.

16. Consecuencias económicas: Ver artículo 23 Imposición de sanciones pecuniarias.

17. Control: Parte del proceso global de control del dopaje que comprende la planificación de distribución de los controles, la recogida de muestras, la manipulación de muestras y su envío al laboratorio.

18. Controles dirigidos: Selección de deportistas específicos para la realización de controles conforme a los criterios establecidos en el Estándar Internacional para Controles e Investigaciones.

19. Convención de la UNESCO: Convención Internacional contra el Dopaje en el Deporte adoptada durante la 33.ª sesión de la Asamblea General de la UNESCO el 19 de octubre de 2005, que incluye todas y cada una de las enmiendas adoptadas por los Estados Parte firmantes de la Convención y por la Conferencia de las Partes signatarias de la Convención Internacional contra el Dopaje en el Deporte.

20. Culpabilidad: Cualquier incumplimiento de una obligación o ausencia de la adecuada atención a una situación concreta. Entre los factores que deben tomarse en consideración al evaluar el grado de culpabilidad del deportista u otra persona están, por ejemplo, su experiencia, si se trata de una persona protegida, consideraciones especiales como la discapacidad, el grado de riesgo que debería haber sido percibido por el deportista y el grado de atención e investigación aplicados por el mismo en relación con lo que debería haber sido el nivel de riesgo percibido. Al evaluar el grado de culpabilidad del deportista u otra persona, las circunstancias analizadas deben ser específicas y pertinentes para explicar la desviación de estos del patrón de conducta esperado. Así, por ejemplo, el hecho de que un deportista vaya a perder la oportunidad de ganar grandes cantidades de dinero durante un periodo de sanción, o de que quede poco tiempo para que finalice su carrera deportiva, o la programación del calendario deportivo, no serían factores relevantes a tener en cuenta para reducir el periodo de sanción con arreglo al artículo 26 de la presente ley.

21. Deporte de equipo: Deporte que autoriza la sustitución de jugadores durante una competición.

22. Deporte individual: Cualquier deporte que no sea de equipo.

23. Deportista: Cualquier persona que haya obtenido una licencia deportiva o se encontrare en proceso de obtenerla o tuviese expectativas de solicitarla.

24. Deportista aficionado: Deportista que no es de nivel nacional ni internacional. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte tiene potestad para aplicar las normas antidopaje a un deportista aficionado. En relación con estos deportistas, la organización antidopaje podrá elegir entre: realizar controles limitados o no realizarlos en absoluto; no utilizar la totalidad de la relación de sustancias prohibidas al analizar las muestras; no requerir información, o requerir información limitada, sobre la localización; o no requerir una autorización terapéutica por adelantado. Sin embargo, si un deportista sobre el cual una organización antidopaje ha decidido ejercer su competencia de control y que compite a un nivel inferior al nacional o internacional, comete una infracción de las normas antidopaje, contempladas en el artículo 20, letras a), c) o d), habrán de aplicarse las sanciones previstas en la presente ley.

25. Divulgación pública o comunicación pública: Ver «Consecuencias de la infracción de las normas antidopaje».

26. Duración de un evento: Tiempo transcurrido entre el principio y el final de un evento, según establezca el organismo responsable del mismo.

27. Educación: Proceso de aprendizaje para trasmitir valores y desarrollar conductas que fomenten y protejan el espíritu deportivo, y para prevenir el dopaje intencionado y no intencionado.

28. En competición: Significa que el período comienza desde las 23:59 horas del día anterior a celebrarse una competición en la que el deportista tenga previsto participar hasta el final de dicha competición y el proceso de recogida de muestras relacionado con ella.

29. Evento deportivo: Serie o parte de las competiciones que se desarrollan bajo la dirección de un único organismo deportivo que adopta las reglas de participación y organización del mismo.

Por el ámbito territorial en el que se desarrollan pueden clasificarse en:

– Evento internacional: Un evento o competición en el que el Comité Olímpico Internacional, el Comité Paralímpico Internacional, una federación internacional, la Organización Responsable de Grandes Eventos u otra organización deportiva internacional actúan como organismo responsable del evento o nombran a los delegados técnicos del mismo.

– Evento nacional: Un evento o competición que no sea internacional, independientemente de que participen deportistas de nivel nacional o internacional.

30. Fuera de competición: Todo periodo que no sea en competición.

31. Grupo Registrado de Control: Grupo de deportistas de la más alta prioridad identificados separadamente a nivel internacional por las federaciones internacionales y a nivel nacional por la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte, que están sujetos a la vez a controles específicos, en competición y fuera de competición, en el marco de la planificación de distribución de los controles de dicha federación internacional o comisión y que están obligados a proporcionar información acerca de su localización conforme al artículo 11 de esta ley.

32. Independencia institucional: Los miembros del Comité Sancionador Antidopaje en fase de resolución de recursos tendrán plena independencia institucional de la organización antidopaje encargada de la gestión de resultados, por lo que no deberán estar en modo alguno sometidos a su autoridad.

33. Independencia operacional: La instrucción de los procedimientos debe ser llevada a cabo por personas no miembros del Comité Sancionador Antidopaje. Los miembros del Comité Sancionador Antidopaje llevarán a cabo los procesos de audiencia y resolución sin injerencias de la organización antidopaje o de terceros.

34. Límite de decisión: Valor del resultado para una sustancia umbral en una muestra, por encima del cual se notificará un resultado analítico adverso según lo definido en la Norma Internacional para Laboratorios.

35. Lista de Sustancias y Métodos Prohibidos: Lista aprobada por Resolución de la Presidencia del Consejo Superior de Deportes y publicada en el Boletín Oficial del Estado, de acuerdo con los compromisos internacionales asumidos por España, y, en particular, de la Convención Antidopaje de la UNESCO, en la que constan todas las sustancias y los métodos que están prohibidos en el deporte y cuyo consumo o utilización pueden dar lugar a una sanción por dopaje.

36. Manipulación fraudulenta: Conducta intencional que altera el proceso de control del dopaje, pero que no se incluiría en otro caso en la definición de métodos prohibidos. Se considerará manipulación fraudulenta, entre otras conductas, ofrecer o aceptar sobornos con el fin de realizar o dejar de realizar una acción, evitar la recogida de una muestra, influir en el análisis de una muestra o hacerlo imposible, falsificar documentos presentados a una organización antidopaje, comité de autorizaciones de uso terapéutico o tribunal de expertos, obtener falsos testimonios de testigos o cometer cualquier otro acto fraudulento ante la organización antidopaje o la instancia de audiencia para influir en la gestión de los resultados o en la imposición de sanciones, y cualquier otra injerencia, o tentativa de injerencia, similar e intencionada en cualquier aspecto del control del dopaje.

37. Marcador: Un compuesto, un grupo de compuestos o variable(s) biológica(s) que indican el uso de una sustancia prohibida o de un método prohibido.

38. Menor: Persona física que no ha alcanzado la edad de dieciocho años.

39. Metabolito: Cualquier sustancia producida por un proceso de biotransformación.

40. Método específico: Cualquier método descrito como tal en la Lista de Sustancias y Métodos Prohibidos. Ningún método prohibido se considerará método específico, a menos que figure específicamente como tal en la lista de prohibiciones.

41. Método prohibido: Cualquier método descrito como tal en la Lista de Sustancias y Métodos Prohibidos.

42. Muestra: Cualquier material biológico recogido con fines de control del dopaje.

43. Nivel mínimo a efectos de notificaciones: La concentración estimada de una sustancia prohibida o de uno o varios de sus metabolitos o marcadores en una muestra, por debajo de la cual los laboratorios acreditados por la AMA no deben notificar un resultado analítico adverso en relación con esa muestra.

44. Norma Internacional: Norma adoptada por la Agencia Mundial Antidopaje en apoyo del Código. El respeto de la Norma Internacional (en contraposición a otra norma, práctica o procedimiento alternativo) bastará para determinar que se han ejecutado correctamente los procedimientos previstos en la Norma Internacional.

Entre las Normas Internacionales se incluirá cualquier documento Técnico publicado de acuerdo con dicha Norma Internacional.

45. Organización Antidopaje: La Agencia Mundial Antidopaje o un signatario que es responsable de la adopción de normas para iniciar, poner en práctica o exigir el cumplimiento de cualquier parte del proceso de control del dopaje. Esto incluye, por ejemplo, al Comité Olímpico Internacional, al Comité Paralímpico Internacional, a otras organizaciones responsables de grandes eventos deportivos que realizan controles en eventos de los que sean responsables, a la Agencia Mundial Antidopaje, a las federaciones internacionales, y a las organizaciones nacionales antidopaje.

46. Organización Nacional Antidopaje: La o las entidades designadas por cada país como autoridad principal responsable de la adopción y la puesta en práctica de normas antidopaje, de la recogida de muestras, de la gestión de los resultados, y de la tramitación del procedimiento sancionador, a nivel nacional. En España es la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte.

47. Organizaciones Responsables de Grandes Eventos: Las asociaciones continentales de Comités Olímpicos Nacionales y otras organizaciones multideportivas internacionales que funcionan como organismo rector de un evento continental, regional o internacional.

48. Participante: Cualquier deportista o personal de apoyo al deportista.

49. Pasaporte Biológico del Deportista: El programa y métodos de recogida y cotejo de datos descrito en la Norma Internacional para Controles e Investigaciones y en la Norma Internacional para Laboratorios de la Agencia Mundial Antidopaje.

50. Persona: Una persona física o una organización u otra entidad.

51. Persona Protegida: Deportista u otra persona física (i) que en el momento de la infracción de las normas antidopaje no ha alcanzado la edad de dieciséis años; (ii) que en el momento de la infracción de las normas antidopaje no ha alcanzado la edad de dieciocho años y no está incluido en ningún grupo de seguimiento ni ha competido nunca en un evento internacional en categoría abierta *(open);* (iii) carente de capacidad jurídica o de obrar por razones distintas a la edad.

52. Personal de apoyo a los y las deportistas: Cualquier entrenador, preparador físico, director deportivo, agente, directivo, personal del club deportivo o equipo, o profesional o personal sanitario o paramédico, familiar o cualquier otra persona que trabaje con, trate o ayude a deportistas que participen en o se preparen para competiciones deportivas.

53. Posesión: Posesión física o de hecho (que sólo se determinará si la persona ejerce o pretende ejercer un control exclusivo de la sustancia o método prohibidos o del lugar en el que se encuentren la sustancia o método prohibidos); dado, sin embargo, que si la persona no ejerce un control exclusivo de la sustancia o método prohibido o del lugar en el que se encuentre la sustancia o método prohibido, la posesión de hecho solo se apreciará si la persona tuviera conocimiento de la presencia de la sustancia o método prohibido y tenía la intención de ejercer un control sobre él; por lo tanto, no podrá haber infracción de las normas antidopaje sobre la base de la mera posesión si, antes de recibir cualquier notificación que le comunique una infracción de las normas antidopaje, la persona ha tomado medidas

concretas que demuestren que ya no tiene voluntad de posesión y que ha renunciado a ella declarándolo explícitamente ante una organización antidopaje. Sin perjuicio de cualquier otra afirmación en contrario recogida en esta definición, la compra (incluso por medios electrónicos o de otra índole) de una sustancia o método prohibido constituye posesión por parte de la persona que realice dicha compra.

54. Programa de Observadores Independientes: Equipo de observadores y/o auditores, bajo la supervisión de la AMA, que observa y orienta sobre el proceso de control del dopaje antes o durante determinados eventos y comunica sus observaciones como parte del programa de supervisión del cumplimiento de la AMA.

55. Producto contaminado: Un producto que contiene una sustancia prohibida que no está descrita en la etiqueta del producto ni en la información disponible en una búsqueda razonable en Internet.

56. Responsabilidad del Deportista: A los efectos de lo previsto en los apartados a) y b) del artículo 20 de la ley, correrá a cargo del deportista probar la ausencia de culpa o negligencia, o el error de hecho o de derecho en que hubiera podido incurrir en el uso o consumo de la sustancia o método prohibido. A los efectos del apartado j) del artículo 20 de la ley, en relación con los apartados b) y e) del mismo artículo correrá a cargo del deportista probar la inexistencia de tentativa en la comisión de las conductas descritas.

57. Resultado Adverso en el Pasaporte: Un informe identificado como un Resultado Adverso en el Pasaporte descrito en las Normas Internacionales de la Agencia Mundial Antidopaje aplicables.

58. Resultado Analítico Adverso: Un informe por parte de un laboratorio acreditado o aprobado por la Agencia Mundial Antidopaje que, de conformidad con la Norma Internacional para Laboratorios identifique en una muestra la presencia de una sustancia prohibida o de sus metabolitos o marcadores o evidencias del uso de un método prohibido.

59. Resultado Anómalo: Informe emitido por un laboratorio acreditado o aprobado por la Agencia Mundial Antidopaje que requiere una investigación más detallada según la Norma Internacional para Laboratorios de la Agencia Mundial Antidopaje o los documentos técnicos relacionados antes de decidir sobre la existencia de un Resultado Analítico Adverso.

60. Resultado Anómalo en el Pasaporte: Un informe identificado como un Resultado Anómalo en el Pasaporte descrito en las Normas Internacionales de la Agencia Mundial Antidopaje, aplicables.

61. Sede de un evento: Cada una de las sedes designadas por la autoridad responsable del evento.

62. Signatarios: Aquellas entidades firmantes del Código Mundial Antidopaje y que acepten implementar el Código, de acuerdo con lo previsto en el artículo 23 del Código Mundial Antidopaje.

63. Sistema de información establecido por la Agencia Mundial Antidopaje: Herramienta para la gestión de bases de datos, situada en un sitio web para introducir información, almacenarla, compartirla y elaborar informes con el fin de ayudar a las partes interesadas y a la Agencia Mundial Antidopaje en sus actividades contra el dopaje, de acuerdo con la legislación relativa a la protección de datos. Dicho sistema recibe el nombre, en la actualidad, de «Anti-Doping Administration and Management System (ADAMS)».

64. Suspensión provisional: Ver Consecuencias de la Infracción de las Normas Antidopaje.

65. Suspensión: Ver Consecuencias de la Infracción de las Normas Antidopaje.

66. Sustancia de abuso: Cualquier sustancia descrita como tal en la Lista de Sustancias y Métodos Prohibidos. Las sustancias de abuso incluyen las sustancias prohibidas que figuran específicamente como tales en la lista de prohibiciones porque en la sociedad se abusa de ellas con frecuencia en contextos distintos de los deportivos.

67. Sustancia específica: Cualquier sustancia descrita como tal en la Lista de Sustancias y Métodos Prohibidos. Todas las sustancias prohibidas se considerarán sustancias específicas, salvo que se indique en la lista de prohibiciones.

68. Sustancia prohibida: Cualquier sustancia o grupo de sustancias descrita como tal en la Lista de Sustancias y Métodos Prohibidos. La determinación por parte de la AMA de las sustancias prohibidas y los métodos prohibidos que se incluirán en la lista de prohibiciones, la clasificación de las sustancias en las categorías de dicha lista, la clasificación de una

sustancia como prohibida siempre o solo durante la competición y la clasificación de una sustancia o método como sustancia específica, método específico o sustancia de abuso, es definitiva y no podrá ser impugnada por ningún deportista u otra persona, sobre la base, entre otras alegaciones, de que la sustancia o método no es un agente enmascarante, no tiene el potencial de mejorar el rendimiento deportivo, no representa un riesgo para la salud o no vulnera el espíritu deportivo.

69. Tentativa: Conducta voluntaria que constituye un paso sustancial en el curso de una acción planificada cuyo objetivo es la comisión de una infracción de normas antidopaje. No obstante, no habrá infracción de las normas antidopaje basada únicamente en esta tentativa de cometer tal infracción si la persona desiste antes de ser descubierta por un tercero no implicado en la misma.

70. Tercero delegado: Toda persona en la que una organización antidopaje delegue algún aspecto del control del dopaje o los programas educativos en materia antidopaje, incluidos, entre otros, terceros u otras organizaciones antidopaje que lleven a cabo la recogida de muestras u otros servicios de control del dopaje o programas de educación antidopaje para la organización antidopaje, o individuos que actúen en calidad de contratistas independientes y lleven a cabo servicios de control del dopaje para la organización antidopaje (por ejemplo, agentes o asistentes de control antidopaje que no sean empleados). Esta definición no incluye al Tribunal de Arbitraje Deportivo.

71. Tráfico: La venta, entrega, transporte, envío, reparto o distribución (o la posesión con cualquiera de estos fines) de una sustancia prohibida o método prohibido (ya sea físicamente o por medios electrónicos o de otra índole) por parte de un deportista, el personal de apoyo al deportista o cualquier otra persona sometida a la jurisdicción de una organización antidopaje a cualquier tercero; no obstante, esta definición no incluye las acciones de buena fe que realice el personal médico en relación con una sustancia prohibida utilizada para propósitos terapéuticos genuinos y legales u otra justificación aceptable, y no incluirá acciones relacionadas con sustancias prohibidas que no estén prohibidas fuera de competición, a menos que las circunstancias en su conjunto demuestren que la finalidad de dichas sustancias prohibidas no sea para propósitos terapéuticos genuinos y legales o que tengan por objeto mejorar el rendimiento deportivo.

72. Tribunal Administrativo del Deporte: Órgano de ámbito estatal, adscrito orgánicamente al Consejo Superior de Deportes que actúa con independencia de éste, creado en virtud del artículo 84 de la Ley 10/1990, de 15 de octubre, del Deporte.

73. Tribunal de Arbitraje Deportivo: Institución independiente para la solución de controversias relacionadas con el deporte a través del arbitraje o la mediación por medio de normas de procedimiento adaptadas a las necesidades específicas del mundo del deporte.

74. Uso: La utilización, aplicación, ingestión, inyección o consumo por cualquier medio de una sustancia prohibida o de un método prohibido.

§ 82

Real Decreto 792/2023, de 24 de octubre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte. [Inclusión parcial]

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 255, de 25 de octubre de 2023
Última modificación: 24 de diciembre de 2024
Referencia: BOE-A-2023-21845

[. . .]

TÍTULO PRELIMINAR

Disposiciones generales

[. . .]

Artículo 3. *Protección de datos de carácter personal.*

El tratamiento de los datos de carácter personal a que se refiere el presente reglamento se ajustará a las disposiciones establecidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como por las demás normas que adapten el derecho español a la normativa europea y será conforme a lo dispuesto en la disposición adicional cuarta de la Ley Orgánica 11/2021, de 28 de diciembre.

[. . .]

TÍTULO I

Autorizaciones de uso terapéutico

[. . .]

Artículo 11. *Registro de las AUT.*

1. Las AUT que se concedan, junto con la documentación complementaria correspondiente, deberán registrarse en el sistema de información ADAMS, quedando bajo la custodia de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte.

2. Los datos relativos a las AUT de los que disponga la CELAD se suprimirán de acuerdo con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, y el Reglamento (UE)

2016/679, una vez transcurridos diez años de acuerdo con lo dispuesto en la Ley Orgánica 11/2021, de 28 de diciembre.

No obstante lo anterior, los formularios de solicitud y la información médica complementaria, así como cualquier otra información relativa a la AUT que no se mencione expresamente en el Estándar Internacional para la Protección de la Privacidad y la Información Personal se eliminarán transcurridos doce meses.

Artículo 11. *AUT con carácter retroactivo.*

1. La persona deportista que necesite utilizar una sustancia o método prohibidos, por motivos terapéuticos, deberá solicitar y obtener una AUT antes de utilizar o poseer la sustancia o el método en cuestión, salvo los casos en los que se cumpla al menos una de las siguientes condiciones:

a) Necesidad de tratamiento urgente o de emergencia de una afección médica, de acuerdo a las guías de práctica clínica actualizadas basadas en la evidencia.

b) Concurrencia de circunstancias excepcionales que impidan al deportista presentar –o al CAUT considerar– una solicitud de AUT antes de la recogida de muestras;

c) Uso, por parte de la persona deportista, fuera de competición, por razones terapéuticas, una sustancia que solo está prohibida en competición.

d) Concurrencia de otras circunstancias excepcionales, y sin perjuicio de cualquier otra previsión en el ISTUE, en las que fuera manifiestamente injusto no conceder una AUT retroactiva, siempre y cuando la AMA conceda una aprobación previa, tanto en el caso de personas deportistas de nivel internacional como de nivel nacional, excepto en el caso de personas deportistas aficionadas, si bien, en este último caso, la decisión del CAUT podrá ser revisada en cualquier momento por la AMA, pudiendo ser revocada por esta.

2. Si la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte decide tomar una muestra de una persona deportista aficionada, que no es ni de nivel internacional ni nacional, y esta está usando una sustancia o método prohibido por razones terapéuticas, debe permitir a la persona deportista solicitar una AUT con carácter retroactivo.

3. El cumplimiento de una de las excepciones anteriores no conlleva la concesión directa de la AUT, que, en todo caso, será evaluada conforme a los criterios establecidos en el artículo 8.

4. En todos los supuestos, junto con la solicitud de AUT deberá remitirse la documentación que acredite la causa por la que se solicita con dicho carácter retroactivo.

[. . .]

TÍTULO III

Control del dopaje

CAPÍTULO I

Planificación de controles

[. . .]

Artículo 18. *Base de datos de control del dopaje.*

1. Los datos relativos al Plan de Distribución de Controles formarán parte de la base de datos de control del dopaje, que será supervisada y administrada por la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte.

2. De conformidad con la disposición adicional cuarta de la Ley Orgánica 11/2021, de 28 de diciembre, esta base de datos se tratará de acuerdo con lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

3. A tal efecto, se incluirán en la base de datos de control del dopaje:

a) Los datos que permitan la identificación y comunicación con las personas deportistas susceptibles de ser sometidas a los controles que la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte determine, y en particular, el domicilio, una cuenta de correo electrónico y un número de teléfono en el que pueda comunicarse con ellas, así como cualesquiera otros datos complementarios que faciliten esta comunicación.

b) El Plan de Distribución de Controles.

c) Los datos relacionados con los controles de dopaje realizados.

d) La relación de Agentes de control del dopaje habilitados, así como el estado y las vicisitudes de sus respectivas habilitaciones.

e) Cualquier otra información relativa a la persona deportista, aportada por terceros o conocida por la autoridad competente como resultado de sus propias investigaciones, que pudiera resultar útil o relevante a los efectos de su seguimiento y control.

[. . .]

CAPÍTULO III

Realización de controles

Sección 1.ª Disposiciones generales

[. . .]

Artículo 23. *Horas de descanso nocturno.*

(Suprimido).

[. . .]

Artículo 27. *Coordinación con otras Organizaciones Antidopaje.*

1. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte considerará plenamente válidos a los efectos previstos en la Ley Orgánica 11/2021, de 28 de diciembre, y en el presente reglamento, los controles de dopaje realizados por personal que se encuentre habilitado por las Federaciones Internacionales o por las Organizaciones Antidopaje reconocidas por la Agencia Mundial Antidopaje.

2. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte coordinará sus esfuerzos con otras Organizaciones Antidopaje, con el fin de evitar controles de dopaje repetitivos e innecesarios a las personas deportistas.

3. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte compartirá la información sobre los controles con otras organizaciones antidopaje, a través del sistema de información establecido por la Agencia Mundial Antidopaje, en los términos y condiciones establecidos en la normativa aplicable, y con pleno respeto a la normativa vigente sobre protección de datos.

[. . .]

Sección 5.ª Notificación a la persona deportista

[. . .]

Artículo 41. *Información a la persona deportista.*

Una vez contrastada la identidad, la persona que practique la notificación informará a la persona deportista de las siguientes circunstancias:

a) Que ha sido seleccionada para someterse a un control de dopaje.

b) Cuál es el organismo responsable de la realización del control.

c) El tipo de muestra a obtener.

d) El derecho a estar acompañada por una persona debidamente identificada durante el proceso de recogida de muestras.

e) El derecho a solicitar información adicional coherente y adecuada sobre la recogida de muestras.

f) El derecho a no someterse a la prueba si existe alguna causa que constituya justificación válida para ello, de acuerdo con lo dispuesto en el artículo 15.4 de la Ley Orgánica 11/2021, de 28 de diciembre.

g) La obligatoriedad de someterse al control si no existe causa que constituya justificación válida para no hacerlo, a riesgo de incurrir, en caso contrario, en la infracción tipificada en el artículo 20.c) de la Ley Orgánica 11/2021, de 28 de diciembre.

h) La obligación de permanecer en todo momento bajo la observación de alguno de los componentes del equipo de recogida de muestras designados para ello, desde la notificación hasta la finalización del proceso de recogida de muestras.

i) La obligación de identificarse en cualquier momento ante el miembro del equipo de recogida de muestras que lo solicite y mediante documentación oficial que confirme su identidad e incluya fotografía.

j) Cuando se trate de una persona deportista con discapacidad, el derecho a solicitar las adaptaciones necesarias que estén justificadas.

k) La obligación de presentarse en el área del control de dopaje o en el lugar indicado para la recogida de muestras en las condiciones que indique la notificación.

l) El derecho a solicitar una demora para presentarse en el área de control de dopaje, según lo previsto en el artículo 42.

m) Se le facilitará la información acerca del tratamiento de sus datos personales y los derechos que le asisten, conforme a lo señalado en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD) y la Ley Orgánica 3/2018, de 20 de junio.

n) El derecho a manifestar por escrito en el formulario de Control de Dopaje cuantas circunstancias, hechos o comentarios relativos al proceso de toma de muestras que considere relevantes o que convengan a su derecho.

[. . .]

CAPÍTULO IV

Pasaporte Biológico de la persona deportista

Artículo 48. *El Pasaporte Biológico como medio de control del dopaje.*

1. El Pasaporte Biológico de la persona deportista implica el seguimiento longitudinal de marcadores biológicos, al objeto de detectar cambios en sus parámetros biológicos susceptibles de ser causados por el uso de sustancias prohibidas y/o práctica de métodos prohibidos.

Dichos marcadores serán seleccionados específicamente para la detección del uso de un determinado grupo de sustancias y/o métodos.

2. El Programa de Pasaporte Biológico formará parte del Plan de Distribución de Controles. A todas las personas deportistas que son sometidas a controles de dopaje se les elaborará un Pasaporte Biológico con los datos obtenidos a partir de los controles realizados.

3. De conformidad con la disposición adicional cuarta de la Ley Orgánica 11/2021, de 28 de diciembre, la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte será la responsable de la custodia y la gestión de los datos integrados en el Pasaporte Biológico, cuyo régimen seguirá lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 7/2021, de 26 de mayo.

4. El Programa de Pasaporte Biológico tendrá el contenido, estructura, módulos, datos e informes que determine el correspondiente ISTI y el Estándar Internacional de Gestión de Resultados de la Agencia Mundial Antidopaje, debiendo observarse en su seguimiento y elaboración las reglas y normas establecidas en ellos.

[. . .]

TÍTULO IV

Del Comité Sancionador Antidopaje

[. . .]

Artículo 56. *Resoluciones de los procedimientos sancionadores.*

1. Las resoluciones del Comité Sancionador Antidopaje sobre expedientes sancionadores previstas en la Ley Orgánica 11/2021, de 28 de diciembre, incluirán los votos particulares, si los hubiere, y serán firmadas con identificación de nombre y apellidos por la persona encargada de la ponencia y la persona titular de la Secretaría del Comité, con el visto bueno del presidente.

2. Las resoluciones sancionadoras del Comité Sancionador Antidopaje serán dictadas respetando el derecho al honor y la intimidad de las personas, así como lo dispuesto en la legislación de Protección de Datos de Carácter Personal.

3. Las resoluciones de los procedimientos sancionadores serán publicadas de acuerdo con lo dispuesto en el artículo 44 de la Ley Orgánica 11/2021, de 28 de diciembre.

TÍTULO V

Procedimiento para la imposición de sanciones disciplinarias en materia de dopaje

[. . .]

CAPÍTULO II

Tramitación del procedimiento sancionador

[. . .]

Sección 3.ª Instrucción

[. . .]

Artículo 69. *Efectos de las sanciones.*

1. La imposición de sanciones relacionadas con el dopaje en el deporte, incluyendo la suspensión provisional, constituye un supuesto de imposibilidad para obtener o ejercer los derechos derivados de todas las licencias deportivas de que fuese titular, cualquiera que sea su naturaleza, tipo o duración, en cualquier ámbito territorial, en los términos previstos en el artículo 49.9 de la Ley 39/2022, de 30 de diciembre, del Deporte y en los términos previstos en el artículo 10 del Código Mundial Antidopaje.

2. Durante el período de inhabilitación o suspensión provisional, la persona sancionada no podrá participar, en calidad alguna, en ninguna competición o actividad autorizada u organizada por alguno de los signatarios de la Convención de la Unesco o de los signatarios del Código Mundial Antidopaje, organización miembro de algún Signatario, o un club u otra organización miembro de un Signatario, ni tampoco en competiciones autorizadas u organizadas por las ligas profesionales u organizadores de eventos nacionales o internacionales o actividades deportivas de nivel nacional o de élite financiada con fondos públicos, sea cual sea la modalidad o especialidad deportiva en la que quiera participar.

La persona sancionada podrá solicitar de la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte la autorización para participar en programas educativos o de rehabilitación.

3. El cómputo de las sanciones impuestas se hará en la forma prevista en el artículo 30 de la Ley Orgánica 11/2021, de 28 de diciembre.

4. Las sanciones personales de multa, en los casos de personas deportistas, solo podrán imponerse cuando estos obtengan o hayan obtenido ingresos que estén asociados a la

actividad deportiva desarrollada. La obtención de tales ingresos podrá acreditarse por el órgano sancionador por cualquiera de los medios admitidos en derecho.

5. La Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte interesará de las entidades concedentes la recuperación del apoyo financiero otorgado a cualquier persona sancionada por la comisión de cualquier infracción de las normas antidopaje, así como de cualesquiera otras ventajas económicas o beneficios fiscales relacionados con su práctica deportiva que pudiera obtener de aquellas.

6. Las sanciones impuestas por los órganos disciplinarios competentes son inmediatamente ejecutivas para la persona interesada y para todas aquellas llamadas a ejecutarlas desde la fecha en que se les notifique la resolución sancionadora, salvo que el órgano que deba conocer de los recursos contra dicha resolución acuerde su suspensión. Las suspensiones de las licencias surtirán efecto por el mero hecho de su notificación en forma a las personas afectadas, sin necesidad de actos concretos de ejecución.

7. Las resoluciones firmes que impongan sanciones por la comisión de las infracciones previstas en el artículo 20 de la Ley Orgánica 11/2021, de 28 de diciembre, serán objeto de publicación de conformidad con lo establecido en el artículo 14 del Código Mundial Antidopaje.

No obstante, en el caso de que afecten a personas menores de edad, personas protegidas, o personas deportistas aficionadas, las resoluciones sancionadoras no se publicarán a menos que razonadamente se valore la conveniencia de proceder a la publicación atendiendo a la pertinencia de la misma y las circunstancias del caso. Asimismo, cuando las personas presten la colaboración a que se refiere el artículo 34 de la Ley Orgánica 11/2021, de 28 de diciembre, podrá exceptuarse la publicación de la sanción en los términos previstos en el artículo 10.7.1 del Código Mundial Antidopaje.

La publicación únicamente contendrá el nombre y apellidos de la persona infractora, especialidad deportiva, precepto vulnerado, sustancia o método empleados y sanción impuesta. Esta publicación no podrá mantenerse más de un mes o mientras dure el período de la sanción si este fuera superior.

Será objeto de publicación la adopción de las medidas de suspensión provisional, si bien en estos casos la publicación únicamente contendrá la identidad de la persona infractora.

Para proceder a la publicación se utilizarán medios electrónicos. En todo caso, esta publicación deberá ajustarse a lo dispuesto en la disposición adicional séptima de la Ley Orgánica 3/2018, de 5 de diciembre, así como a lo dispuesto en el artículo 14 del Código Mundial Antidopaje.

8. Cuando como consecuencia del trámite de audiencia o de recurso interpuesto contra la resolución sancionadora se determinase la inexistencia de la infracción imputada a la persona deportista o a otra persona, o se redujera la sanción impuesta, se procederá a la publicación de la estimación de dicho recurso, siempre que la persona deportista o dicha otra persona otorgare su consentimiento a dicha publicación. En tal caso, la Agencia Estatal Comisión Española para la Lucha Antidopaje en el Deporte divulgará la decisión de manera íntegra o redactándola de una forma aceptable para la persona deportista o la otra persona. En todo caso, se atenderá a lo dispuesto en el artículo 13 y 14 del CMA.

[. . .]

§ 83

Ley 19/2021, de 20 de diciembre, por la que se establece el ingreso mínimo vital. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 304, de 21 de diciembre de 2021
Última modificación: 22 de mayo de 2024
Referencia: BOE-A-2021-21007

[. . .]

CAPÍTULO III

Acción protectora

[. . .]

Artículo 23. *Cesión de datos y confidencialidad de los mismos.*

1. En el suministro de información en relación con los datos de carácter personal que se deba efectuar a la Administración de la Seguridad Social para la gestión de esta prestación, será de aplicación lo previsto en los apartados 1 y 2 del artículo 71 del texto refundido de la Ley General de la Seguridad Social, aprobado por Real Decreto Legislativo 8/2015, de 30 de octubre. El suministro de información no requerirá el consentimiento previo del interesado, ni de las personas que formen parte de la unidad de convivencia, por ser un tratamiento de datos de los referidos en los artículos 6.1.e) y 9.2.h) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

2. Todas las personas y todos los organismos que intervengan en cualquier actuación referente al ingreso mínimo vital quedan obligados a la reserva de datos en los términos establecidos en el artículo 77 del texto refundido de la Ley General de la Seguridad Social.

3. Las administraciones públicas actuantes tomarán las medidas oportunas para que, en el curso del procedimiento administrativo, quede garantizada la confidencialidad de los datos suministrados por los solicitantes para la gestión de la prestación y estarán obligadas a cumplir con la legislación vigente en materia de protección de datos.

4. Las resoluciones de las prestaciones de ingreso mínimo vital se comunicarán por el Instituto Nacional de la Seguridad Social, sin necesidad del consentimiento previo del titular de los datos personales, a las comunidades autónomas y entidades locales a través de la adhesión a los procedimientos informáticos con los requisitos establecidos por el Instituto Nacional de la Seguridad Social, con la finalidad de facilitar la información estrictamente necesaria para el reconocimiento y control de las prestaciones competencia de dichas administraciones. La información facilitada no podrá ser utilizada con ninguna otra finalidad

si no es con el consentimiento del interesado. Todo ello en aplicación de los artículos 5.1.b) y c) y 6 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y del artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En las condiciones establecidas en el párrafo anterior, se comunicarán las resoluciones de las prestaciones del ingreso mínimo vital a los órganos competentes de la Administración General del Estado, de las comunidades autónomas y, en su caso, a las corporaciones locales, para la realización de aquellas actividades que, en el marco de la colaboración y cooperación, deban realizar dichas administraciones, en materia de gestión y control del ingreso mínimo vital que corresponde al Instituto Nacional de la Seguridad Social.

Asimismo, en las condiciones establecidas en el primer párrafo, el Instituto Nacional de la Seguridad Social podrá comunicar de forma telemática, sin el consentimiento previo del titular de los datos personales, la información que resulte necesaria sobre el ingreso mínimo vital a las instituciones y organismos públicos que lo soliciten para que puedan realizar, dentro del ámbito de sus competencias, actuaciones derivadas de la aplicación del ingreso mínimo vital.

5. La Secretaría General de Objetivos y Políticas de Inclusión y Previsión Social podrá comunicar a las administraciones públicas, entidades del tercer sector de acción social y agentes sociales con los que suscriba acuerdos o convenios para la realización de actuaciones en el marco de las estrategias de inclusión de las personas beneficiarias, de forma telemática y sin el consentimiento previo del titular de los datos personales, la información de contacto de las personas beneficiarias del ingreso mínimo vital candidatas a participar en la actuación, por ser un tratamiento de datos de los referidos en el artículo 6.1 e) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Asimismo, las administraciones públicas, entidades del tercer sector de acción social y agentes sociales con las que la Secretaría General de Objetivos y Políticas de Inclusión y Previsión Social suscriba acuerdos o convenios para el desarrollo y evaluación de estrategias de inclusión, podrán suministrar los datos necesarios de los participantes en las estrategias de inclusión para el diseño, seguimiento y la evaluación de las actuaciones, sin que requiera el consentimiento previo del interesado, por ser igualmente un tratamiento de datos de los referidos en los artículos 6.1.e) y 9.2.h) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Para la recogida y cesión de datos especialmente protegidos y recogidos en el artículo 9.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, será necesaria la autorización expresa e informada de la persona beneficiaria.

La Secretaría General de Objetivos y Políticas de Inclusión y Previsión Social garantizará, mediante la puesta en marcha de un mecanismo accesible para los beneficiarios, que estos pueden ejercer sus derechos de acceso, rectificación, oposición, supresión, limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas, recogidos igualmente en la legislación, de todos aquellos datos especialmente protegidos.

[. . .]

§ 84

Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley Orgánica 8/1980, de 22 de septiembre, de Financiación de las Comunidades Autónomas y otras disposiciones conexas y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 181, de 29 de julio de 2022
Última modificación: sin modificaciones
Referencia: BOE-A-2022-12644

[. . .]

CAPÍTULO II

Acceso al Fichero de Titularidades Financieras por parte de las autoridades competentes

[. . .]

Artículo 5. *Condiciones para el acceso y la consulta.*

1. El acceso y la consulta al Fichero de Titularidades Financieras sólo podrán ser realizados, caso por caso, por personal específicamente designado y autorizado para realizar estas tareas a través de los puntos únicos de acceso establecidos por las autoridades competentes, en los términos que se determinan en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, y en su Reglamento.

2. Este personal, en todo caso, estará debidamente cualificado, tendrá un elevado nivel de integridad y observará unas estrictas normas profesionales de confidencialidad y protección de datos personales.

3. Se adoptarán aquellas medidas técnicas y organizativas necesarias a fin de garantizar la seguridad de los sistemas y los datos a efectos del acceso y consulta de esta información, a fin de hacer frente a los posibles riesgos y amenazas de ciberseguridad atendiendo, en particular, a las normas y recomendaciones que le sean de aplicación, tanto en el ámbito europeo como nacional.

[. . .]

CAPÍTULO III

Intercambio de información y análisis financieros

Artículo 7. *Solicitudes de información dirigidas al Servicio Ejecutivo de la Comisión por parte de las autoridades competentes.*

1. El Servicio Ejecutivo de la Comisión cooperará con las autoridades competentes designadas en el apartado 2 del artículo 3 y responderá a las solicitudes de información financiera que obren en su poder y de análisis financieros ya realizados. En el caso de información financiera, el plazo de respuesta a las solicitudes será de 72 horas desde su recepción. Cuando las solicitudes requieran o se refieran a análisis financieros, se responderán a la mayor brevedad posible.

Las solicitudes de información estarán debidamente motivadas en función de la necesidad y de las circunstancias del caso y tendrán como finalidad la prevención, detección, investigación o enjuiciamiento de delitos graves.

2. El Servicio Ejecutivo de la Comisión no atenderá estas solicitudes cuando concurran motivos objetivos por los que el traslado de la información solicitada podría resultar perjudicial para las investigaciones o los análisis en curso. Tampoco atenderá estas solicitudes en circunstancias excepcionales, cuando la transmisión de la información pudiera ser manifiestamente desproporcionada respecto de los intereses legítimos de una persona física o jurídica, o resulte irrelevante respecto al propósito para el que se haya solicitado.

3. La utilización de la información financiera o del análisis financiero con fines distintos de los originalmente aprobados estará sujeta a la autorización previa del Servicio Ejecutivo de la Comisión, que atenderá las solicitudes efectuadas con arreglo al apartado 1, salvo que concurra alguna de las circunstancias del apartado 2, lo que deberá ser debidamente motivado.

4. La decisión de proceder a la transmisión de la información corresponderá al Servicio Ejecutivo de la Comisión, que motivará de manera adecuada toda negativa a atender una solicitud de información.

5. Las autoridades competentes designadas en el apartado 2 del artículo 3 podrán tratar la información financiera y los análisis financieros recibidos del Servicio Ejecutivo de la Comisión para fines específicos dirigidos a la prevención, detección, investigación y enjuiciamiento de los delitos graves, distintos de los fines para los que los datos personales incluidos en la información o los análisis hayan sido recogidos, de acuerdo con lo establecido en el artículo 6.3 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

[. . .]

CAPÍTULO IV

Protección de datos de carácter personal

Artículo 12. *Protección de datos de carácter personal.*

1. El tratamiento de datos de carácter personal, en aplicación de esta ley, estará a lo dispuesto en el artículo 32 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales y, en lo que resulte de aplicación, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. En el ámbito de aplicación de esta ley se podrán tratar categorías especiales de datos personales cuando sea necesario para cumplir con los fines del artículo 1. En las solicitudes

de información se motivará esta necesidad y solo se accederá a la misma en los supuestos en los que tal circunstancia pueda acreditarse.

3. El tratamiento de categorías especiales de datos personales efectuado por las autoridades competentes y por el Servicio Ejecutivo de la Comisión en el marco del intercambio de información y análisis financiero, así como el realizado en virtud del intercambio de información y de análisis financieros con la participación de la Unidad Nacional de Europol, únicamente podrá ser llevado a cabo por las personas que estén sometidas a un deber específico de confidencialidad y reserva, que hayan recibido una formación específica y sean individualmente autorizadas para ello. Este tratamiento se realizará de conformidad con las normas aplicables en materia de protección de datos, de acuerdo con las orientaciones del delegado de protección de datos designado por la autoridad competente, y será igualmente aplicable a los datos de los menores de edad o a los antecedentes penales.

4. No obstante, cuando ese tratamiento de categorías especiales de datos personales se realice por órganos judiciales y fiscalías en actuaciones o procedimientos de su competencia, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales, se regirá por lo dispuesto en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, las leyes procesales que le sean aplicables y, en su caso, por la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

Artículo 13. *Registro de solicitudes de información.*

1. Las autoridades competentes y el Servicio Ejecutivo de la Comisión deberán llevar un registro de solicitudes de información realizadas al amparo de esta ley, donde figurará, como mínimo, la información siguiente:

a) El nombre y los datos de contacto de la organización y del miembro del personal que hayan solicitado la información y, en la medida de lo posible, el nombre y los datos de contacto del destinatario de los resultados de la búsqueda o la consulta.

b) La referencia al asunto para el que se solicita la información.

c) El objeto de las solicitudes.

d) Cualquier medida de ejecución de las solicitudes.

2. Los registros se conservarán durante un período de 5 años desde que hayan sido realizados y se utilizarán solamente a efectos de comprobar la legalidad del tratamiento, controlar el cumplimiento de las medidas y de las políticas de protección de datos, así como de garantizar la integridad y la seguridad de los datos personales.

Dichos registros estarán a disposición de la autoridad de protección de datos competente a solicitud de ésta, de conformidad con las potestades establecidas en su normativa específica.

Artículo 14. *Elaboración de estadísticas.*

El Servicio Ejecutivo de la Comisión y las autoridades competentes, a fin de evaluar la eficacia de los sistemas de lucha contra los delitos graves de los Estados miembros, elaborarán la información estadística oportuna y completa relativa al cumplimiento de esta ley, que se facilitará a la Comisión Europea con una periodicidad anual y que incluirá al menos:

a) El número de consultas efectuadas por las autoridades competentes al Fichero de Titularidades Financieras de conformidad con el artículo 4 de esta ley.

b) El número de solicitudes cursadas por cada autoridad competente incluida en esta ley; el seguimiento dado a dichas solicitudes; el número de asuntos investigados; el número de personas enjuiciadas; y el número de personas condenadas por delitos graves, cuando se disponga de esta información.

c) La información sobre el tiempo de respuesta del Servicio Ejecutivo de la Comisión y de las autoridades competentes a las solicitudes que reciban, desde su recepción.

d) La información sobre el coste de los recursos humanos o tecnológicos dedicados a las solicitudes tanto nacionales como internacionales cursadas en aplicación de esta ley, en caso de que fuera posible.

[. . .]

§ 85

Ley 20/2022, de 19 de octubre, de Memoria Democrática. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 252, de 20 de octubre de 2022
Última modificación: sin modificaciones
Referencia: BOE-A-2022-17099

[. . .]

Disposición adicional décima. *Protección de datos de carácter personal.*

1. Los tratamientos de datos personales regulados en la presente ley se llevarán a cabo conforme a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Los derechos de acceso, rectificación y supresión se ejercitarán conforme a la normativa referida en el párrafo anterior, sin perjuicio de las especificidades que se recojan en su caso en los apartados siguientes.

2. El tratamiento de los datos personales relativos al registro de víctimas a que se refiere el artículo 9.1 tendrá por finalidad la recopilación de datos de las víctimas que se relacionan en el artículo 3.1, con el objeto de gestionar las políticas públicas de reparación moral y recuperación de la memoria de las víctimas reconocidas en esta ley.

Responsable y base jurídica del tratamiento: Es responsable del tratamiento el departamento que asuma las competencias en materia de conservación, defensa, fomento y divulgación de Memoria Democrática con el fin de garantizar la efectividad de los principios de verdad, justicia, reparación y no repetición, y al objeto de poder desarrollar sus funciones.

La base jurídica del tratamiento es el interés público con fines de archivo, de investigación científica o histórica y con fines estadísticos, así como de gestión de las políticas públicas de memoria democrática para el reconocimiento de las víctimas y la garantía de la efectividad de los principios de verdad, justicia, reparación y no repetición.

En el caso de las investigaciones científicas e históricas y de los datos personales de autoridades y funcionarios públicos relacionados con el ejercicio de sus funciones que revistan un claro interés público, la publicación de dichos datos no es contraria a la normativa de protección de datos de carácter personal.

Minimización de datos: Los datos recogidos se limitarán a los propiamente identificativos, a la represión padecida, del fallecimiento o desaparición de acuerdo con el artículo 3.1, así como el lugar y la fecha en que ocurrieron los hechos, de ser posible, ponderándose que no

se imposibilite u obstaculice gravemente el logro de los fines científicos. Los datos de las personas y entidades que en su caso suministren datos se limitarán a su nombre o denominación y contacto.

Fuentes y exactitud de los datos: Los datos personales serán recabados de archivos, de bases de datos documentales y obras de referencia especializadas suministrados por las diferentes administraciones públicas y por los organismos y entidades del sector público institucional, víctimas, organizaciones memorialistas, grupos de investigación universitarios y cualquier otra fuente, nacional o internacional, que cuente con información relevante para el mismo.

El responsable del tratamiento garantizará la exactitud de los datos tanto por la fuente de procedencia en virtud de lo establecido en la normativa de aplicación al patrimonio documental, como por aplicación para los facilitados por otras fuentes de un proceso de verificación historiográfica.

Transparencia: en virtud de la referida procedencia de los datos obtenidos, las obligaciones de información a los interesados a efectos de lo dispuesto en el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se ajustarán al hecho de que la misma sea conocida por el interesado cuando hubiera sido facilitada por el mismo.

Cuando la información no se hubiera obtenido de los interesados se informará en los términos del artículo 14 del Reglamento (UE) 2016/679, salvo que la comunicación de esta información resulte imposible o suponga un esfuerzo desproporcionado, por referirse a tratamientos con fines de investigación histórica o estadísticos, en cuyo caso se adoptarán las medidas adecuadas para hacerla pública, y específicamente en la página web del Ministerio competente se realizará la publicación o las formas de acceder a esa información.

Conservación y seguridad de los datos: en virtud de la finalidad del tratamiento, la conservación de los datos será indefinida, conforme a la Ley de Patrimonio Histórico Español.

El responsable del tratamiento garantizará la aplicación de las medidas de seguridad correspondientes en cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Ejercicio de derechos: las personas vinculadas a las víctimas fallecidas podrán solicitar el acceso y rectificación de los datos personales de su familiar conforme al artículo 3.1 de la Ley Orgánica 3/2018, de 5 de diciembre. Se limita la posibilidad de supresión de los datos con fundamento al interés público de este tratamiento, y en particular, el derecho de las víctimas y la sociedad en general, a que se garantice la verificación de los hechos y la revelación pública y completa de los motivos y circunstancias en que se cometieron las violaciones del Derecho Internacional Humanitario o de violaciones graves y manifiestas de las normas internacionales de los derechos humanos ocurridas con ocasión de la Guerra y de la Dictadura y, en caso de fallecimiento o desaparición, acerca de la suerte que corrió la víctima, y al esclarecimiento de su paradero.

En virtud del artículo 2.1.b) de la Ley Orgánica 3/2018, de 5 de diciembre, no estarán sujetos a la normativa de protección de datos los datos correspondientes a las víctimas fallecidas.

El ejercicio de derechos para las personas físicas sujetas a la normativa de protección de datos se garantizará conforme a la normativa general de protección de datos.

3. El tratamiento de los datos personales relativos al censo de víctimas regulado en los apartados 2 y 3 del artículo 9 tendrá por finalidad la recopilación de datos de las víctimas de la Guerra y la Dictadura fallecidas o desaparecidas declaradas fallecidas durante la Dictadura franquista, con base en el interés público de investigación histórica y fines estadísticos para el reconocimiento de las víctimas, la recuperación de la memoria personal, familiar y colectiva que facilite el derecho a la verdad recogido en esta ley.

Los datos del censo, que serán de acceso público, serán recabados del registro al que se refiere el apartado anterior, siendo una explotación del mismo, y regirán por ello lo dispuesto en el mismo en cuanto a limitación de datos inscritos, la conservación de los mismos y las obligaciones de información a los interesados.

El responsable del tratamiento será el Ministerio competente en materia de memoria, que garantizará la aplicación de las medidas de seguridad preceptivas, teniendo en cuenta que

dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Las personas vinculadas a las víctimas fallecidas podrán solicitar el acceso y rectificación de los datos personales de su familiar conforme al artículo 3.1 de la Ley Orgánica 3/2018, de 5 de diciembre. Se limita la posibilidad de supresión de los datos con fundamento al interés público de este tratamiento, y en particular, el derecho de las víctimas y la sociedad en general, a que se garantice la verificación de los hechos y la revelación pública y completa de los motivos y circunstancias en que se cometieron las violaciones del Derecho Internacional Humanitario o de violaciones graves y manifiestas de las normas internacionales de los derechos humanos ocurridas con ocasión de la Guerra y de la Dictadura y, en caso de fallecimiento o desaparición, acerca de la suerte que corrió la víctima, y al esclarecimiento de su paradero.

4. El tratamiento de los datos personales relativos al Banco de ADN regulado en el artículo 23, basado en el interés público de investigación histórica y aplicación de las medidas comprendidas en la ley para la búsqueda de desaparecidos e identificación de víctimas, tendrá por finalidad la recepción y almacenamiento de los perfiles de ADN a fin de poder compararlos para la identificación genética de las víctimas de la Guerra y la Dictadura franquista.

Se inscribirán en la base de datos los patrones identificativos obtenidos a partir del ADN en los procedimientos de identificación de restos cadavéricos hallados en fosas o de averiguación de personas desaparecidas que proporcionen, exclusivamente, información genética reveladora de la identidad de la persona y de su sexo.

Los identificadores obtenidos a partir del ADN, respecto de los que se desconozca la identidad de la persona a la que corresponden, permanecerán inscritos en tanto se mantenga dicho anonimato. Una vez identificados, se aplicará lo dispuesto en este artículo a efectos de su cancelación.

Para la recogida de muestras biológicas de familiares y almacenamiento y custodia de las mismas, con carácter previo a la toma de la muestra, la persona donante, familiar de la víctima, deberá firmar el consentimiento para que la misma le sea tomada, informándosele en ese trámite sobre el alcance del tratamiento y los aspectos recogidos en los párrafos siguientes.

El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los datos de identificadores obtenidos a partir del ADN de familiares se podrá efectuar en los términos establecidos en la normativa de protección de datos de carácter personal.

Los datos sólo podrán ser utilizados para la investigación y la identificación genética de restos humanos de personas desaparecidas en la guerra española. Los datos se conservarán mientras sean necesarios para la finalización de los correspondientes procedimientos.

Las muestras o vestigios tomados respecto de los que deban realizarse análisis biológicos, se remitirán a los laboratorios debidamente acreditados. Sólo podrán realizar análisis del ADN para identificación genética en los casos contemplados en esta ley los laboratorios acreditados a tal fin por la Comisión Nacional para el uso forense del ADN que superen los controles periódicos de calidad a que deban someterse.

El responsable del tratamiento será el Instituto Nacional de Toxicología y Ciencias Forenses, que garantizará la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

5. El tratamiento de los datos relativos a la base de datos a que se refiere el artículo 39.3 de la presente ley tiene como fundamento el cumplimiento de una obligación legal que corresponde al Ministerio competente en materia de memoria democrática.

Estos datos sólo serán comunicados a las administraciones públicas en el ejercicio de sus competencias, cuando sea necesario para la tramitación y resolución de sus procedimientos, y se limitarán al número de identificación fiscal.

El responsable del tratamiento será el Ministerio competente en materia de memoria democrática, que garantizará la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los datos de identificadores se podrá efectuar en los términos establecidos en la normativa de protección de datos de carácter personal.

[. . .]

§ 86

Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 44, de 21 de febrero de 2023
Última modificación: sin modificaciones
Referencia: BOE-A-2023-4513

[. . .]

TÍTULO II

Sistema interno de información

CAPÍTULO I

Disposiciones generales

[. . .]

Artículo 5. *Sistema interno de información.*

1. El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por esta ley será el responsable de la implantación del Sistema interno de información, previa consulta con la representación legal de las personas trabajadoras, y tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales.

2. El Sistema interno de información, en cualquiera de sus fórmulas de gestión, deberá:

a) Permitir a todas las personas referidas en el artículo 3 comunicar información sobre las infracciones previstas en el artículo 2.

b) Estar diseñado, establecido y gestionado de una forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado.

c) Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.

d) Integrar los distintos canales internos de información que pudieran establecerse dentro de la entidad.

e) Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad u organismo con el objetivo de que el primero en conocer la posible irregularidad sea la propia entidad u organismo.

f) Ser independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades u organismos, sin perjuicio de lo establecido en los artículos 12 y 14.

g) Contar con un responsable del sistema en los términos previstos en el artículo 8.

h) Contar con una política o estrategia que enuncie los principios generales en materia de Sistemas interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo.

i) Contar con un procedimiento de gestión de las informaciones recibidas.

j) Establecer las garantías para la protección de los informantes en el ámbito de la propia entidad u organismo, respetando, en todo caso, lo dispuesto en el artículo 9.

Artículo 6. *Gestión del Sistema interno de información por tercero externo.*

1. La gestión del Sistema interno de información se podrá llevar a cabo dentro de la propia entidad u organismo o acudiendo a un tercero externo, en los términos previstos en esta ley. A estos efectos, se considera gestión del Sistema la recepción de informaciones.

2. La gestión del sistema por un tercero externo exigirá en todo caso que este ofrezca garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones.

La existencia de corresponsables del tratamiento de datos personales requiere la previa suscripción del acuerdo regulado en el artículo 26 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. La gestión del Sistema interno de información por un tercero no podrá suponer un menoscabo de las garantías y requisitos que para dicho sistema establece esta ley ni una atribución de la responsabilidad sobre el mismo en persona distinta del Responsable del Sistema previsto en el artículo 8.

4. El tercero externo que gestione el Sistema tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales. El tratamiento se regirá por el acto o contrato al que se refiere el artículo 28.3 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Artículo 7. *Canal interno de información.*

1. Todo canal interno de información de que disponga una entidad para posibilitar la presentación de información respecto de las infracciones previstas en el artículo 2 estará integrado dentro del Sistema interno de información a que se refiere el artículo 5.

2. El canal interno deberá permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas. La información se podrá realizar bien por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto, o verbalmente, por vía telefónica o a través de sistema de mensajería de voz. A solicitud del informante, también podrá presentarse mediante una reunión presencial dentro del plazo máximo de siete días.

En su caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo a lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Además, a quienes realicen la comunicación a través de canales internos se les informará, de forma clara y accesible, sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

Las comunicaciones verbales, incluidas las realizadas a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz, deberán documentarse de alguna de las maneras siguientes, previo consentimiento del informante:

a) mediante una grabación de la conversación en un formato seguro, duradero y accesible, o

b) a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

Sin perjuicio de los derechos que le corresponden de acuerdo a la normativa sobre protección de datos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

3. Los canales internos de información permitirán incluso la presentación y posterior tramitación de comunicaciones anónimas.

4. Los canales internos de información podrán estar habilitados por la entidad que los gestione para la recepción de cualesquiera otras comunicaciones o informaciones fuera del ámbito establecido en el artículo 2, si bien dichas comunicaciones y sus remitentes quedarán fuera del ámbito de protección dispensado por la misma.

[. . .]

TÍTULO VI

Protección de datos personales

Artículo 29. *Régimen jurídico del tratamiento de datos personales.*

Los tratamientos de datos personales que deriven de la aplicación de esta ley se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, y en el presente título.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

Artículo 30. *Licitud de los tratamientos de datos personales.*

1. Se considerarán lícitos los tratamientos de datos personales necesarios para la aplicación de esta ley.

2. El tratamiento de datos personales, en los supuestos de comunicación internos, se entenderá lícito en virtud de lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, cuando, de acuerdo a lo establecido en los artículos 10 y 13 de la presente ley, sea obligatorio disponer de un sistema interno de información.

Si no fuese obligatorio, el tratamiento se presumirá amparado en el artículo 6.1.e) del citado reglamento.

3. El tratamiento de datos personales en los supuestos de canales de comunicación externos se entenderá lícito en virtud de lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.

4. El tratamiento de datos personales derivado de una revelación pública se presumirá amparado en lo dispuesto en los artículos 6.1.e) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.

5. El tratamiento de las categorías especiales de datos personales por razones de un interés público esencial se podrá realizar conforme a lo previsto en el artículo 9.2.g) del Reglamento (UE) 2016/679.

Artículo 31. *Información sobre protección de datos personales y ejercicio de derechos.*

1. Cuando se obtengan directamente de los interesados sus datos personales se les facilitará la información a que se refieren los artículos 13 del Reglamento (UE) 2016/679 del

Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 3/2018, de 5 de diciembre.

A los informantes y a quienes lleven a cabo una revelación pública se les informará, además, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

2. La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.

3. Los interesados podrán ejercer los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

4. En caso de que la persona a la que se refieran los hechos relatados en la comunicación o a la que se refiera la revelación pública ejerciese el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

Artículo 32. *Tratamiento de datos personales en el Sistema interno de información.*

1. El acceso a los datos personales contenidos en el Sistema interno de información quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

a) El Responsable del Sistema y a quien lo gestione directamente.

b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.

c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen.

e) El delegado de protección de datos.

2. Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones a las que se refiere el artículo 2, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley.

Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

3. Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

4. En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

5. Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco de los Sistemas de información a que se refiere el presente artículo.

Artículo 33. *Preservación de la identidad del informante y de las personas afectadas.*

1. Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas.

2. Los sistemas internos de información, los canales externos y quienes reciban revelaciones públicas no obtendrán datos que permitan la identificación del informante y deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

3. La identidad del informante solo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

Las revelaciones hechas en virtud de este apartado estarán sujetas a salvaguardas establecidas en la normativa aplicable. En particular, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente lo comunique al informante, le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión.

Artículo 34. *Delegado de protección de datos.*

De acuerdo con lo que dispone el artículo 37.1.a) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Autoridad Independiente de Protección del Informante, A.A.I., y las autoridades independientes que en su caso se constituyan, deberán nombrar un delegado de protección de datos.

[. . .]

§ 87

Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 303, de 20 de diciembre de 2023
Última modificación: 3 de enero de 2025
Referencia: BOE-A-2023-25758

LIBRO PRIMERO

Medidas de Eficiencia Digital y Procesal del Servicio Público de Justicia

TÍTULO PRELIMINAR

Disposiciones generales

Artículo 1. *Objeto y principios.*

1. El presente libro tiene por objeto regular la utilización de las tecnologías de la información por parte de los ciudadanos y ciudadanas y los y las profesionales en sus relaciones con la Administración de Justicia y en las relaciones de la Administración de Justicia con el resto de administraciones públicas, y sus organismos públicos y entidades de derecho público vinculadas y dependientes.

2. En la Administración de Justicia se utilizarán las tecnologías de la información de acuerdo con lo dispuesto en el presente real decreto-ley, asegurando la seguridad jurídica digital, el acceso, autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, conservación, portabilidad e interoperabilidad de los datos, informaciones y servicios que gestione en el ejercicio de sus funciones.

3. Las tecnologías de la información en el ámbito de la Administración de Justicia tendrán carácter instrumental de soporte y apoyo a la actividad jurisdiccional, con pleno respeto a las garantías procesales y constitucionales.

Artículo 2. *Ámbito de aplicación.*

El presente real decreto-ley será de aplicación a la Administración de Justicia, a los ciudadanos y ciudadanas en sus relaciones con ella y a los y las profesionales que actúen en su ámbito, así como a las relaciones entre aquélla y el resto de administraciones públicas, y sus organismos públicos y entidades públicas vinculadas y dependientes.

Las referencias generales a los ciudadanos y ciudadanas efectuadas en este real decreto-ley comprenden a las personas jurídicas y otras entidades sin personalidad jurídica, salvo en los casos en que la misma norma especifique otra cosa. Las referencias generales a los y las profesionales comprenden a las personas que ejercen la Abogacía, la Procura y a los Graduados y Graduadas Sociales, entre otros profesionales, salvo en los casos en que la misma norma especifique otra cosa.

Artículo 3. *Terminología.*

A los efectos del presente real decreto-ley, los términos utilizados en el mismo tendrán el significado que en su caso se determine en el propio real decreto-ley o en su anexo final.

Artículo 4. *Servicios electrónicos de la Administración de Justicia.*

1. En los términos previstos en este real decreto-ley, las administraciones públicas con competencia en medios materiales y personales de la Administración de Justicia garantizarán la prestación del servicio público de Justicia por medios digitales equivalentes, interoperables y con niveles de calidad equiparables, que aseguren en todo el territorio del Estado, al menos, los siguientes servicios:

a) La itineración de expedientes electrónicos y la transmisión de documentos electrónicos entre cualesquiera órganos y oficinas judiciales, fiscalía europea, u oficinas fiscales.

b) La interoperabilidad de datos entre cualesquiera órganos judiciales o fiscales, a los fines previstos en las leyes.

c) La conservación y acceso a largo plazo de los expedientes y documentos electrónicos.

d) La presentación de escritos y comunicaciones dirigidas a los órganos, oficinas judiciales y oficinas fiscales a través de un registro común para toda la Administración de Justicia, de manera complementaria e interoperable con los registros judiciales electrónicos que correspondan a una o varias oficinas judiciales en los distintos ámbitos de competencia, para aquellos usuarios externos a estos ámbitos de competencia.

e) Un Punto de Acceso General de la Administración de Justicia.

f) Un servicio personalizado, de acceso a los distintos servicios, procedimientos e informaciones accesibles de la Administración de Justicia que afecten a un ciudadano o ciudadana cuando sean parte o interesados legítimos y directos en un procedimiento o actuación judicial. A dicho servicio podrán ser accesibles a través de un servicio central, a través de las respectivas Sedes Judiciales Electrónicas de cada uno de los territorios, o a través de ambos sistemas.

g) Un registro común de datos para el contacto electrónico de ciudadanos, ciudadanas y profesionales, interoperable con los posibles registros existentes, para facilitar el contacto de los usuarios en los distintos ámbitos de competencias.

h) El acceso por parte de los y las profesionales a través de un punto común a todos los actos de comunicación de los que sean destinatarios, cualquiera que sea el órgano judicial u oficina fiscal que los haya emitido. Dicho acceso podrá realizarse a través de un punto común, a través de las respectivas Sedes Judiciales Electrónicas de cada uno de los territorios, o a través de ambos sistemas.

i) El Tablón Edictal Judicial Único.

j) Portales de datos en los términos previstos en el presente real decreto-ley.

k) Un registro interoperable en el que conste el personal al servicio de la Administración de Justicia que haya sido habilitado para la realización de determinados trámites o actuaciones en ella.

l) El Registro Electrónico de Apoderamientos Judiciales.

m) La posible textualización de actuaciones orales registradas en soporte apto para la grabación y reproducción del sonido y la imagen.

n) La identificación y firma de los intervinientes en actuaciones no presenciales.

ñ) Las comunicaciones electrónicas transfronterizas relativas a actuaciones de cooperación jurídica internacional, a través de un nodo común que asegure el cumplimiento de los requisitos de interoperabilidad que se hayan convenido en el marco de la Unión Europea o, en su caso, de la normativa convencional de aplicación.

o) La identificación y firma no criptográfica en las actuaciones y procedimientos judiciales llevados a cabo por videoconferencia, y en los servicios y actuaciones no presenciales.

p) Aquellos otros servicios que se determinen por las administraciones públicas con competencias en medios materiales y personales de la Administración de Justicia, en el marco institucional de cooperación definido en el presente real decreto-ley.

Las condiciones de prestación de estos servicios se aprobarán por el Comité técnico estatal de la Administración judicial electrónica, debiendo cada Administración Pública con competencias en materias de Administración de Justicia determinar si la prestación se realiza a través de servicios comunes, a través de las respectivas sedes electrónicas de cada territorio, o a través de ambos.

2. Los sistemas empleados para la prestación de los servicios serán interoperables entre todos los órganos, oficinas judiciales y oficinas fiscales, Institutos de Medicina Legal, Instituto Nacional de Toxicología y Ciencias Forenses, oficinas de atención a las víctimas del delito y cualesquiera otras que, por razón de sus funciones o competencias, se relacionen directamente con la Administración de Justicia, con independencia del lugar donde estén radicadas.

Asimismo, deberán ser plenamente interoperables con el resto de administraciones públicas, y sus organismos públicos y entidades de derecho público vinculadas y dependientes. Igualmente, todos los sistemas empleados deberán ser plenamente accesibles electrónicamente para quienes se relacionen con la Administración de Justicia.

3. Las administraciones públicas con competencia en medios materiales y personales de la Administración de Justicia habilitarán diferentes canales o medios para la prestación de los servicios electrónicos, asegurando en todo caso y en la forma que estimen adecuada el acceso a los mismos a todos los ciudadanos y ciudadanas, con independencia de sus circunstancias personales, medios o conocimientos.

A estos fines, las administraciones competentes en materia de Justicia contarán, al menos, con los siguientes medios:

a) Oficinas de información y atención al público que, en los procedimientos en los que los ciudadanos y ciudadanas comparezcan y actúen sin asistencia letrada y sin representación procesal, pondrán a su disposición de forma libre y gratuita los medios e instrumentos precisos para ejercer los derechos reconocidos en el artículo 5 de este real decreto-ley, debiendo contar con asistencia y orientación sobre su utilización, bien a cargo del personal de las oficinas en que se ubiquen o bien por sistemas incorporados al propio medio o instrumento.

b) Sedes judiciales electrónicas creadas y gestionadas por las distintas administraciones competentes en materia de Justicia y disponibles para las relaciones de los ciudadanos y ciudadanas con la Administración de Justicia a través de redes de comunicación. Dichas sedes serán interoperables con la Carpeta Justicia y su relación se publicará por la Administración competente.

c) Servicios de atención telefónica con los criterios de seguridad y las posibilidades técnicas existentes, que faciliten a los ciudadanos y ciudadanas las relaciones con la Administración de Justicia en lo que se refiere a los servicios electrónicos mencionados en este precepto.

d) Puntos de información electrónicos, ubicados en los edificios judiciales.

TÍTULO I

Derechos y deberes digitales en el ámbito de la Administración de Justicia

Artículo 5. *Derechos de los ciudadanos y ciudadanas.*

1. Los ciudadanos y ciudadanas tienen derecho a relacionarse con la Administración de Justicia utilizando medios electrónicos para el ejercicio de los derechos previstos en los capítulos I y VII del título III del libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en la forma y con las limitaciones que en los mismos se establecen.

2. Además, los ciudadanos y ciudadanas tienen, en relación con la utilización de los medios electrónicos en la actividad judicial y en los términos previstos en el presente real decreto-ley, los siguientes derechos:

a) A un servicio público de Justicia prestado por medios digitales, en los términos establecidos en los apartados 1 y 3 del artículo 4 de este real decreto-ley.

b) A la igualdad en el acceso electrónico a los servicios de la Administración de Justicia.

c) A la calidad de los servicios públicos prestados por medios electrónicos.

d) A un servicio personalizado de acceso a procedimientos, informaciones y servicios accesibles de la Administración de Justicia en los que sean partes o interesados legítimos.

e) A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con la Administración de Justicia.

f) A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean parte procesal o interesados legítimos, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, y en las leyes procesales.

g) A acceder y obtener copia del expediente judicial electrónico y de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de parte o acrediten interés legítimo y directo, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, y en las leyes procesales.

h) A la conservación por la Administración de Justicia en formato electrónico de los documentos electrónicos que formen parte de un expediente conforme a la normativa vigente en materia de archivos judiciales.

i) A utilizar los sistemas de identificación y firma electrónica ante la Administración de Justicia del documento nacional de identidad, aquellos otros dispositivos puestos a su disposición con la finalidad de facilitar su autenticación o firma de acuerdo con lo establecido el artículo 20 del presente real decreto-ley, así como aquellos otros determinados en la misma.

j) A la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que sean objeto de tratamiento por la Administración de Justicia, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, y con las especialidades establecidas por esta; en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; y en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como los que deriven de leyes procesales.

k) A elegir las aplicaciones o sistemas para relacionarse con la Administración de Justicia siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos y ciudadanas y, en todo caso, siempre que sean compatibles con los que dispongan los órganos judiciales y se respeten las garantías y requisitos previstos en el procedimiento de que se trate.

l) A que las aplicaciones o sistemas para relacionarse telemáticamente con la Administración de Justicia estén disponibles en todas las lenguas oficiales del Estado en los términos previstos en el artículo 231 de la Ley Orgánica 6/1985, de 1 de julio.

3. Las personas jurídicas tienen los derechos reconocidos en el apartado 1 y en las letras a), b), c), d), f), g), h), i), j) y l) del apartado 2 de este artículo. En todo caso, estarán sujetas a las previsiones especiales que el presente real decreto-ley establezca.

Artículo 6. *Derechos y deberes de los y las profesionales que se relacionen con la Administración de Justicia.*

1. Los y las profesionales que se relacionen con la Administración de Justicia tienen derecho a relacionarse con la misma a través de medios electrónicos.

2. Además, respecto de la utilización de los medios electrónicos en la actividad judicial y en los términos previstos en el presente real decreto-ley, los y las profesionales que se relacionen con la Administración de Justicia tienen los siguientes derechos:

a) A acceder y conocer por medios electrónicos el estado de la tramitación de los procedimientos en los que, según conste en el procedimiento judicial, ostenten la representación procesal o asuman la defensa jurídica de parte personada o que haya acreditado interés legítimo y directo, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, y en las leyes procesales.

b) A acceder y obtener copia del expediente judicial electrónico y de los documentos electrónicos que formen parte de procedimientos en los que, según conste en el procedimiento judicial, ostenten la representación procesal o asuman la defensa jurídica de parte personada o que haya acreditado interés legítimo y directo, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, y en las leyes procesales.

c) A acceder en formato electrónico a los documentos conservados por la Administración de Justicia que formen parte de un expediente, según la normativa vigente en materia de archivos judiciales.

d) A utilizar los sistemas de identificación y firma establecidos previstos en el presente real decreto-ley y de conformidad con la misma. A tal efecto, los Consejos Generales o Superiores profesionales correspondientes deberán poner a disposición de los órganos judiciales, oficinas judiciales y oficinas fiscales los protocolos y sistemas de interconexión que permitan el acceso necesario por medios electrónicos al registro de profesionales colegiados ejercientes previsto en el artículo 10 de la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales, garantizando que en él consten sus datos profesionales, tales como nombre y apellidos de los y las profesionales colegiados, número de colegiación, títulos oficiales de los que estén en posesión, domicilio profesional y situación de habilitación profesional, y, en el caso de las sociedades profesionales, la denominación social de la misma, así como los datos de los socios otorgantes y de los y las profesionales que actúan en su seno.

e) A la garantía de la seguridad y confidencialidad y disponibilidad en el tratamiento de los datos personales realizado por la Administración de Justicia que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, y con las especialidades establecidas por esta; en las leyes procesales, en el presente real decreto-ley, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; en la Ley Orgánica 3/2018, de 5 de diciembre; y en la Ley Orgánica 7/2021, de 26 de mayo, así como los que deriven de leyes procesales. Corresponderá a la Administración competente cumplir con las responsabilidades que, como administración prestacional, tenga atribuidas en esa materia.

f) A que los sistemas de información de la Administración de Justicia posibiliten y favorezcan la desconexión digital, de manera que permita la conciliación de la vida laboral, personal y familiar de los y las profesionales que se relacionen con la Administración de Justicia, con respeto a lo dispuesto en la legislación procesal.

Las administraciones con competencias en materia de Justicia deberán definir, mediante convenios y protocolos, los términos, medios y medidas adecuadas, en el ámbito tecnológico, para posibilitar la desconexión, la conciliación y el descanso en los períodos inhábiles procesalmente y en aquellos en que las personas profesionales de la Abogacía, la Procura y los Graduados y Graduadas Sociales estén haciendo uso de las posibilidades dispuestas a tal fin en las normas procesales.

3. Los y las profesionales que se relacionen con la Administración de Justicia, en los términos previstos en el presente real decreto-ley, tienen el deber de utilizar los medios electrónicos, las aplicaciones o los sistemas establecidos por las administraciones competentes en materia de Justicia, respetando en todo caso las garantías y requisitos previstos en el procedimiento que se trate.

4. Las administraciones competentes en materia de Justicia asegurarán el acceso de los y las profesionales a los servicios electrónicos proporcionados en su ámbito a través de puntos de acceso electrónico, consistentes en sedes judiciales electrónicas creadas y gestionadas por aquéllas y disponibles para los y las profesionales a través de redes de comunicación, en los términos previstos en el presente real decreto-ley.

Artículo 7. *Uso obligatorio de medios e instrumentos electrónicos por la Administración de Justicia.*

1. Los órganos y oficinas judiciales, fiscalías, y oficinas fiscales utilizarán para el desarrollo de su actividad y ejercicio de sus funciones los medios técnicos, electrónicos, informáticos y electrónicos puestos a su disposición por la Administración competente, siempre que dichos medios cumplan con los esquemas nacionales de interoperabilidad y seguridad, así como con la normativa técnica, instrucciones técnicas de seguridad, requisitos funcionales fijados por el Comité técnico estatal de la Administración judicial electrónica y normativa de protección de datos personales.

2. Las administraciones públicas con competencia en medios materiales y personales de la Administración de Justicia dotarán a los órganos y oficinas judiciales y oficinas fiscales de sistemas tecnológicos que permitan la tramitación electrónica de los procedimientos y cumplan con los requisitos definidos en el apartado anterior.

3. Las instrucciones de contenido general o singular relativas al uso de las tecnologías que el Consejo General del Poder Judicial o la Fiscalía General del Estado dirijan a los jueces y magistrados o a los fiscales, respectivamente, serán de obligado cumplimiento. Igualmente lo serán las que la persona titular de la Secretaría General de la Administración de Justicia dirija a los letrados de la Administración de Justicia.

TÍTULO II

Acceso digital a la Administración de Justicia

CAPÍTULO I

De la sede judicial electrónica

Artículo 8. *Sede judicial electrónica.*

1. La sede judicial electrónica es aquella dirección electrónica disponible para los ciudadanos y ciudadanas a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a cada una de las administraciones competentes en materia de Justicia.

2. Las sedes judiciales electrónicas se crearán mediante disposición publicada en el «Boletín Oficial del Estado» o el Boletín o Diario Oficial de la Comunidad Autónoma correspondiente, y tendrán, al menos, los siguientes contenidos:

a) Identificación de la dirección electrónica de referencia de la sede, que incluya el nombre del dominio que le otorgue la Administración competente.

b) Identificación de su titular, así como del órgano u órganos administrativos encargados de la gestión y de los servicios puestos a disposición de los ciudadanos, ciudadanas y profesionales en la misma.

c) Identificación de los canales de acceso a los servicios disponibles en la sede, con expresión, en su caso, de los teléfonos y oficinas a través de los cuales también puede accederse a los mismos.

d) Cauces disponibles para la formulación de sugerencias y quejas con respecto al servicio que presta la sede.

e) Acceso al expediente judicial electrónico, a la presentación de escritos, a la práctica de notificaciones y a la agenda de señalamientos e información, de los sistemas habilitados de videoconferencia.

3. El establecimiento de una sede judicial electrónica conlleva la responsabilidad de su titular de garantizar la integridad y actualización de la información facilitada, así como el acceso a los servicios previstos en la misma.

4. Las administraciones competentes en materia de Justicia determinarán las condiciones e instrumentos de creación de las sedes judiciales electrónicas, con sujeción a los principios de publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad.

5. La publicación en las sedes judiciales electrónicas de informaciones, servicios y transacciones respetará los estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos y ciudadanas.

6. Las sedes judiciales electrónicas se regirán, además de por lo previsto en este real decreto-ley, por lo establecido en el artículo 38 de la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público.

7. Las sedes judiciales electrónicas utilizarán comunicaciones cifradas con base en certificados cualificados de autenticación de sitios web o medio equivalente, según lo dispuesto en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

8. Las direcciones electrónicas de la Administración de Justicia que tengan la condición de sedes judiciales electrónicas deberán hacerse constar de forma visible e inequívoca.

9. El instrumento de creación de la sede judicial electrónica será accesible directamente o mediante enlace a su publicación en el «Boletín Oficial del Estado» o en el de la Comunidad Autónoma correspondiente.

10. Los sistemas de información que soporten las sedes judiciales electrónicas deberán asegurar la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de las informaciones que manejan y de los servicios prestados.

Artículo 9. *Características de las sedes judiciales electrónicas y sus clases.*

1. Se realizarán preferentemente a través de sedes judiciales electrónicas las actuaciones, procedimientos y servicios que requieran la autenticación de la Administración de Justicia o de los ciudadanos, ciudadanas y profesionales por medios electrónicos. Dichos servicios podrán ser accesibles desde la Carpeta Justicia en las condiciones establecidas por el Comité técnico estatal de la Administración judicial electrónica, para asegurar la completa y exacta incorporación de la información y accesos publicados en éste.

2. Las sedes judiciales electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

3. Cuando esté justificado por motivos técnicos o funcionales, se podrán crear una o varias sedes judiciales electrónicas derivadas de una sede judicial electrónica. Dichas sedes derivadas deberán resultar accesibles desde la dirección electrónica de la sede principal, sin perjuicio de que sea posible el acceso electrónico directo.

4. Las sedes judiciales electrónicas asociadas se crearán por disposición del órgano administrativo que tenga atribuida esta competencia y deberán cumplir los mismos requisitos de publicidad que las sedes judiciales electrónicas principales.

Artículo 10. *Contenido y servicios de las sedes judiciales electrónicas.*

1. Toda sede judicial electrónica dispondrá, al menos, de los siguientes contenidos:

a) Identificación de la sede, así como de la Administración Pública u organismos titulares y de los responsables de la gestión, de los servicios puestos a disposición en la misma y, en su caso, de las sedes de ella derivadas, así como del órgano, oficina judicial u oficina fiscal que origine la información que se deba incluir en la sede judicial electrónica.

b) Información necesaria para su correcta utilización, incluyendo el mapa de la sede judicial electrónica o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles.

c) Relación de sistemas de identificación y firma electrónica que, conforme a lo previsto en este real decreto-ley, sean admitidos o utilizados en la sede.

d) Normas de creación del registro o registros electrónicos accesibles desde la sede.

e) Información relacionada con la protección de datos de carácter personal, incluyendo un enlace con la sede electrónica de la Agencia Española de Protección de Datos y las de las Agencias Autonómicas de Protección de Datos, asimismo, la información prevista en los artículos 13 y 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y cualquier otra que permita cumplir con el principio de transparencia,

así como el inventario de tratamientos a que hace referencia el artículo 31.2 de la Ley Orgánica 3/2018, de 5 de diciembre.

2. Las sedes judiciales electrónicas tendrán, al menos, los siguientes servicios a disposición de los ciudadanos, ciudadanas y profesionales:

a) La relación de los servicios disponibles en la sede judicial electrónica.
b) La carta de servicios y la carta de servicios electrónicos.
c) La relación de los medios electrónicos que los ciudadanos, ciudadanas y profesionales pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con la Administración de Justicia.
d) Acceso al expediente judicial electrónico, a la presentación de escritos, a la práctica de actos de comunicación y a la agenda de señalamientos e información, en su caso, de los sistemas habilitados de videoconferencia.
e) Un enlace para la formulación de sugerencias y quejas ante los órganos correspondientes.
f) Acceso, en los términos establecidos en las leyes procesales, al estado de la tramitación del expediente.
g) Un enlace al Tablón Edictal Judicial único, como medio de publicación y consulta de las resoluciones y comunicaciones que por disposición legal deban fijarse en el tablón de anuncios o edictos.
h) Verificación de los sellos electrónicos de los órganos u organismos públicos que abarque la sede.
i) Comprobación de la autenticidad e integridad de los documentos emitidos por los órganos u organismos públicos que abarca la sede, que hayan sido autenticados mediante código seguro de verificación.
j) Servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede.
k) La Carta de Derechos de los Ciudadanos ante la Justicia.
l) Enlace al apartado de instrucciones o gestión de cita para la solicitud de asistencia jurídica gratuita.

3. No será necesario recoger en las sedes derivadas la información y los servicios a que se refieren los apartados anteriores cuando ya figuren en la sede de la que aquéllas derivan.
4. La sede judicial electrónica garantizará el régimen de cooficialidad lingüística vigente en su territorio.

Artículo 11. *Regla especial de responsabilidad.*

El órgano que origine la información que se deba incluir en la sede judicial electrónica será el responsable de la veracidad e integridad de su contenido. La sede judicial electrónica establecerá los medios necesarios para que el ciudadano o ciudadana conozca si la información o servicio al que accede corresponde a la propia sede o a un punto de acceso que no tiene el carácter de sede o a un tercero.

Artículo 12. *Punto de Acceso General de la Administración de Justicia.*

1. El Punto de Acceso General de la Administración de Justicia será un portal orientado a los ciudadanos y ciudadanas que dispondrá de su sede electrónica que, como mínimo, contendrá la Carpeta Justicia y el directorio de las sedes judiciales electrónicas que, en este ámbito, faciliten el acceso a los servicios, procedimientos e informaciones accesibles correspondientes a la Administración de Justicia, al Consejo General del Poder Judicial, a la Fiscalía General del Estado y a los organismos públicos vinculados o dependientes de la misma, así como a las administraciones con competencias en materia de Justicia. También podrá proporcionar acceso a servicios o informaciones correspondientes a otras administraciones públicas o corporaciones que representen los intereses de los y las profesionales que se relacionan con la Administración de Justicia, mediante la celebración de los correspondientes convenios.
2. El Punto de Acceso General de la Administración de Justicia será gestionado por el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes conforme a los acuerdos

que se adopten en el Comité técnico estatal de la Administración judicial electrónica, con el objetivo de asegurar la completa y exacta incorporación de la información y accesos publicados en éste, de manera interoperable con los posibles puntos ubicados en los portales habilitados por cada administración competente.

3. El punto de acceso general responderá a los principios de accesibilidad universal y claridad de la información, e incluirá contenidos dirigidos a colectivos vulnerables, especialmente a niños, niñas y adolescentes, que pudieran ser de su interés.

4. El Punto de Acceso General de la Administración de Justicia ofrecerá al ciudadano o ciudadana, al menos, un servicio de consulta de expedientes en los que figure como parte en procedimientos judiciales, y en todo caso la posibilidad de conocer y acceder a recibir las notificaciones de todos los órganos judiciales.

5. Se ofrecerá a las personas jurídicas, cuyo volumen de causas pudiera dificultar una gestión a través del punto de acceso general, sistemas específicos en función de niveles de volumen de expedientes o de áreas de gestión en atención a los referidos acuerdos que se adopten conforme al apartado 2 de este artículo.

CAPÍTULO II

De la Carpeta Justicia

Artículo 13. *La Carpeta en el ámbito de la Administración de Justicia.*

1. La Carpeta Justicia es un servicio personalizado, que facilitará el acceso a los servicios, procedimientos e informaciones accesibles de la Administración de Justicia que afecten a un ciudadano o ciudadana cuando sea parte o justifique un interés legítimo y directo en un procedimiento o actuación judicial. Dicho servicio podrá ofrecerse a través de un sistema común, a través de las respectivas sedes judiciales electrónicas de cada uno de los territorios, o a través de ambos sistemas. Para ello el ciudadano o ciudadana y su profesional autorizado o autorizada deberá identificarse previamente en alguna de las formas previstas en este real decreto-ley.

2. Reglamentariamente, y previo informe del Comité técnico estatal de la Administración judicial electrónica, se establecerán los requisitos que deberá cumplir la Carpeta Justicia en el ámbito de todo el territorio del Estado.

3. De conformidad con los acuerdos que se adopten en el Comité técnico estatal de la Administración judicial electrónica, la Carpeta Justicia será gestionada para asegurar la completa y exacta incorporación de la información y accesos publicados en ésta, bajo responsabilidad del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes.

4. En todo aquello que no esté regulado en este real decreto-ley o en su desarrollo reglamentario, se aplicarán las disposiciones reglamentarias establecidas para la Carpeta Ciudadana del Sector Público Estatal, siempre que por su naturaleza resulten compatibles.

5. La Carpeta Justicia será interoperable con la Carpeta Ciudadana del Sector Público Estatal.

Artículo 14. *Responsabilidad.*

1. Las administraciones públicas con competencias en materia de Justicia velarán por el cumplimiento de los principios de confidencialidad, integridad, autenticidad, trazabilidad, disponibilidad y actualización de la información y los servicios que constituyan la Carpeta Justicia, adoptando las medidas pertinentes para garantizar los mismos.

2. Los ciudadanos y ciudadanas y los y las profesionales están obligados a hacer buen uso de los servicios e informaciones disponibles en la Carpeta Justicia, estando sujetos en caso contrario a las responsabilidades que se deriven de su mal uso.

Artículo 15. *Contenido de la carpeta Justicia.*

1. La Carpeta Justicia deberá contener, como mínimo:

a) La información necesaria que permita a los ciudadanos y ciudadanas su utilización.
b) La relación de los servicios que pueden obtener a través de la misma.
c) Los derechos y obligaciones de los ciudadanos y ciudadanas derivados de su uso.

d) La posibilidad de verificar los accesos previos por el ciudadano o ciudadana.

e) El acceso a los expedientes judiciales en el que el ciudadano fuese parte o interesado, de conformidad con lo establecido en este real decreto-ley.

f) El acceso y firma de los actos de comunicación de la Administración de Justicia pendientes, así como el acceso a los actos de comunicación ya practicados.

g) El acceso a la información personalizada que conste en el Tablón Edictal Judicial Único.

h) La obtención y gestión de cita previa en el ámbito judicial.

i) El acceso a una agenda personalizada de actuaciones ante la Administración de Justicia.

j) El acceso a los cauces para realizar sugerencias y quejas.

Artículo 16. *Acceso de los ciudadanos y ciudadanas a los servicios de la Carpeta Justicia.*

1. Los sistemas informáticos asegurarán que cada vez que el ciudadano o ciudadana acceda a la Carpeta Justicia quede constancia de la información a la que haya accedido, así como de la fecha y hora de dicho acceso.

2. El ciudadano o ciudadana podrá obtener original, copia o justificante, según proceda, de los documentos, resoluciones procesales y judiciales a los que tenga acceso a través de la Carpeta Justicia.

3. El ciudadano o ciudadana podrá canalizar, a través de su Carpeta Justicia, el ejercicio de los derechos previstos en la normativa aplicable en materia de protección de datos de carácter personal.

Artículo 17. *Acceso al expediente judicial electrónico.*

1. La Carpeta Justicia facilitará un servicio de consulta del estado de la tramitación, así como de acceso a todos los expedientes judiciales electrónicos en los que el ciudadano o ciudadana sea parte.

2. En el marco del Comité técnico estatal de la Administración judicial electrónica podrán definirse otros perfiles para el acceso, o la consulta limitada, al estado del procedimiento o a otras informaciones y documentos por quienes, sin ser parte, justifiquen interés legítimo y directo.

3. Los accesos y consultas a los que se refieren los apartados anteriores se ajustarán a lo dispuesto en las leyes procesales, con especial atención a la normativa sobre actuaciones declaradas secretas o reservadas y sobre protección de datos de carácter personal.

4. En el caso de procedimientos judiciales que no se hallen en soporte electrónico, se habilitarán igualmente servicios electrónicos de información que comprendan cuando menos el estado de la tramitación y el órgano judicial competente.

5. A los fines previstos en este artículo, los sistemas de gestión procesal serán interoperables con la Carpeta Justicia en los términos que defina el Comité técnico estatal de la Administración judicial electrónica.

Artículo 18. *Cita previa.*

1. Los ciudadanos y ciudadanas podrán solicitar cita previa ante los órganos y oficinas judiciales y oficinas fiscales a través de la Carpeta Justicia, así como visualizar sus citas previas señaladas en el sistema.

2. Los servicios de cita previa de las Administraciones Públicas con competencias en materias de Administración de Justicia serán interoperables con el servicio de cita previa de la Carpeta Justicia, en los términos que defina el Comité técnico estatal de la Administración judicial electrónica, sin perjuicio de la interoperabilidad que puedan mantener con otros servicios.

CAPÍTULO III

De la identificación y firma electrónicas

Sección 1.ª Disposiciones comunes de los sistemas de identificación y firma

Artículo 19. *Sistemas de identificación admitidos por la Administración de Justicia.*

La identificación en las actuaciones procesales y judiciales se realizará conforme a lo establecido en el artículo 9 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, sin perjuicio del reconocimiento de los sistemas de identificación de otros países con los que la Administración de Justicia haya llegado a un acuerdo, en el marco de lo establecido por la Comisión Europea. Por vía reglamentaria podrán habilitarse otros sistemas de identificación digital.

Artículo 20. *Sistemas de firma admitidos por la Administración de Justicia.*

1. La firma en las actuaciones procesales y judiciales se realizará conforme a lo establecido en el artículo 10 de la Ley 39/2015, de 1 de octubre, y en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, y la Ley 6/2020, de 11 de noviembre, sin perjuicio del reconocimiento de los sistemas de firma de otros países con los que la Administración de Justicia pueda llegar a un acuerdo, en el marco de lo establecido por la Comisión Europea. Por vía reglamentaria podrán habilitarse otros sistemas de firma.

En el marco del Comité técnico estatal de la Administración judicial electrónica podrá determinarse el nivel de firma aplicable en cada una de las actuaciones en el ámbito de la Administración de Justicia. Dicha determinación deberá realizarse en la Guía de Interoperabilidad y Seguridad de autenticación, certificados y firma electrónica, en proporción al nivel de seguridad que se estime necesario para cada clase de actuación.

2. Cuando así lo disponga expresamente la normativa reguladora aplicable, la Administración de Justicia podrá admitir los sistemas de identificación contemplados en este real decreto-ley como sistemas de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los ciudadanos, ciudadanas y de los y las profesionales que se relacionan con la Administración de Justicia.

3. Cuando se utilice un sistema de firma de los previstos en este artículo para relacionarse con la Administración de Justicia, la identidad se entenderá ya acreditada mediante el propio acto de la firma.

Artículo 21. *Sistemas de firma para las personas jurídicas y entidades sin personalidad jurídica.*

Las personas jurídicas y las entidades sin personalidad jurídica podrán utilizar sistemas de firma electrónica con atributo de representante para todos los procedimientos y actuaciones ante la Administración de Justicia, siempre que ello sea conforme con las leyes procesales.

Artículo 22. *Uso de los sistemas de identificación y firma en la Administración de Justicia.*

1. La Administración de Justicia admitirá y requerirá la firma electrónica en todos los casos en que, de conformidad con las leyes procesales, los órganos judiciales requieran la firma, sin perjuicio de lo dispuesto en el artículo 29.1.

2. En los demás casos, para realizar actuaciones o acceder a servicios ante la Administración de Justicia será suficiente acreditar previamente la identidad a través de cualquiera de los medios de identificación previstos en este real decreto-ley.

El régimen de acceso a los servicios electrónicos en el ámbito de la Administración de Justicia para los supuestos de sustitución entre profesionales, así como para la habilitación

de sus empleados, se regulará por la respectiva Administración competente mediante disposiciones reglamentarias.

3. El uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación que sean necesarios de acuerdo con la legislación aplicable.

4. Los órganos de la Administración de Justicia u organismos públicos vinculados o dependientes podrán tratar los datos personales consignados, a los efectos de la verificación de la firma.

Artículo 23. *Sistema de identificación seguro en videoconferencias.*

1. En los casos en que lo determine el juez o jueza o tribunal, representante del Ministerio fiscal o letrado o letrada de la Administración de Justicia que en cada caso dirija las actuaciones y procedimientos judiciales llevados a cabo por videoconferencia, o el personal al servicio de la Administración de Justicia que en ausencia de aquellos atienda la actuación o preste el servicio presencial, se podrá usar un sistema de información para la identificación y firma no criptográfica, en los términos y condiciones de uso establecidos en la regulación sobre identificación digital tanto nacional como de la Unión Europea.

2. El sistema servirá para acreditar ante cualquier órgano u oficina judicial o fiscal la identificación electrónica en el procedimiento judicial.

3. El Ministerio de la Presidencia, Justicia y Relaciones con las Cortes posibilitará la prestación de un servicio ajustado a las características indicadas en este artículo a las administraciones públicas con competencia en medios materiales y personales de la Administración de Justicia que decidan hacer uso del mismo, de conformidad con las condiciones que se determinen en el Comité técnico estatal de la Administración judicial electrónica.

Sección 2.ª Identificación y firma de la Administración de Justicia

Artículo 24. *Sistemas de identificación de la Administración de Justicia.*

La Administración de Justicia podrá identificarse mediante los sistemas de identificación establecidos en el artículo 40 de la Ley 40/2015, de 1 de octubre.

Artículo 25. *Sistemas de firma de la Administración de Justicia.*

1. La Administración de Justicia podrá hacer uso de certificados cualificados de sello electrónico de entidad contemplados en el Reglamento UE n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, asociados a la sede judicial o a otros órganos a los que se adscriba la sede, para generar documentos electrónicos sellados.

2. Para la identificación del ejercicio de la competencia en la actuación judicial automatizada, las administraciones públicas con competencia en medios materiales y personales de la Administración de Justicia podrán hacer uso de los siguientes sistemas de firma electrónica:

a) Certificados cualificados de sello electrónico de Administración Pública, de acuerdo con lo dispuesto en el artículo 42 de la Ley 40/2015, de 1 de octubre, o conforme a lo previsto en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

b) Sistemas de Código Seguro de Verificación.

3. El uso de los certificados a que se refiere el apartado anterior deberá incluir la información necesaria para determinar el ámbito organizativo, territorial o de la propia naturaleza de la actuación.

Artículo 26. *Sistemas de Código Seguro de Verificación.*

1. Las administraciones públicas con competencias en medios materiales y personales de la Administración de Justicia podrán gestionar sistemas de Código Seguro de Verificación que, cuando figuren en un documento electrónico o en su versión impresa, permitan el cotejo de la autenticidad e integridad del documento. El cotejo de los documentos con Código

Seguro de Verificación se realizará en la sede judicial electrónica correspondiente al órgano que emitió el documento.

2. La inclusión de Códigos Seguros de Verificación en los documentos se acompañará de la dirección electrónica en la que poder realizar el cotejo.

3. Los Códigos Seguros de Verificación se codificarán de conformidad con los términos que se definan en el marco del Comité técnico estatal de la Administración judicial electrónica.

4. Se podrán establecer requisitos restrictivos de identificación o similares sobre algunos documentos, para evitar que sean accesibles únicamente por su Código Seguro de Verificación, cuando existan razones de protección de la información.

5. Se podrán habilitar mecanismos que ofrezcan el documento en una versión anonimizada. Los documentos electrónicos podrán contener medidas de seguridad tales como marcas de agua, sistemas anti-copia o versiones personalizadas de documentos que permitan detectar la persona concreta que hubiera difundido un documento de forma no autorizada.

Artículo 27. *Sistemas de firma de quienes prestan servicio en la Administración de Justicia.*

1. En los casos en los que el presente real decreto-ley no disponga otra cosa, la identificación y autenticación actuación del órgano u oficina fiscal, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano u oficina o funcionario o funcionaria público, de acuerdo con lo dispuesto en los siguientes apartados.

2. El Comité técnico estatal de la Administración judicial electrónica determinará los sistemas de firma que deben utilizar los y las fiscales, letrados y letradas de la Administración de Justicia y demás personal al servicio de la Administración de Justicia. Dichos sistemas podrán identificar de forma conjunta al titular y el cargo. Los sistemas de firma electrónica de jueces, juezas, magistrados y magistradas serán determinados y provistos por el Consejo General del Poder Judicial. Este podrá establecer, a través de convenios, que el proveedor sea la Administración competente.

3. Las administraciones públicas, en el ámbito de sus competencias, dotarán de sistemas de firma electrónica que cumplan lo previsto en el presente real decreto-ley a quienes tengan atribuida la defensa y representación del Estado y del sector público, a los que se refiere el artículo 551 de la Ley Orgánica 6/1985, de 1 de julio.

Sección 3.ª Interoperabilidad, identificación y representación de los ciudadanos y ciudadanas

Artículo 28. *Admisión de los sistemas de firma e identificación electrónica notificados a la Comisión Europea.*

Sin perjuicio de la obligación de firma electrónica prevista en el artículo 27.1 de este real decreto-ley para todos los casos en que proceda conforme a las leyes procesales, la Administración de Justicia admitirá todos los sistemas de firma e identificación electrónica incluidos en la lista publicada por la Comisión Europea en el «Diario Oficial de la Unión Europea» a la que se refiere el apartado 2 del artículo 9 del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Artículo 29. *Identificación de los ciudadanos y ciudadanas por funcionario o funcionaria público.*

1. En los supuestos en que para la realización de cualquier actuación por medios electrónicos se requiera la identificación del ciudadano o ciudadana en los términos previstos en este real decreto-ley, y estos no dispongan de tales medios, la identificación y autenticación podrá ser válidamente realizada por personal funcionario público habilitado al efecto, mediante el uso del sistema de firma electrónica del que esté dotado.

2. Para la eficacia de lo dispuesto en el apartado anterior, el ciudadano o ciudadana deberá identificarse y prestar su consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.

3. Si la constancia se obtiene utilizando una firma, esta podrá ser manuscrita, bien en papel, bien utilizando dispositivos técnicos idóneos para su captura que gestionen la firma con medidas de seguridad equivalentes a la firma avanzada definida en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, y según lo establecido en la Guía de Interoperabilidad y Seguridad de Autenticación, Certificados y Firma Electrónica aprobada por el Comité técnico estatal de la Administración judicial electrónica.

Artículo 30. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre administraciones con competencias en materia de Justicia, órganos y entidades de derecho público serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en el presente artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a la Administración de Justicia, el Comité técnico estatal de la Administración judicial electrónica determinará las condiciones y garantías por las que se regirán, que al menos comprenderán la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas administraciones o a entidades de derecho público, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio.

4. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

TÍTULO III

De la tramitación electrónica de los procedimientos judiciales

CAPÍTULO I

Disposiciones comunes e inicio del procedimiento

Artículo 31. *Integridad y registro de actividad.*

1. Los sistemas de información y comunicación empleados por la Administración de Justicia conservarán un registro de las actividades de tratamiento conforme a lo dispuesto en la normativa sobre protección de datos. Además, deberán mantener registros de, al menos, las siguientes operaciones de tratamiento en sistemas de tratamiento automatizados: recogida, alteración, consulta, comunicación, incluidas las transferencias, y combinación o supresión. Los registros harán posible determinar la justificación, la fecha y la hora de tales operaciones, así como la persona que realiza la consulta o comunicación de los datos personales y la identidad de los destinatarios o destinatarias de dichos datos.

2. Las funcionalidades a las que se refiere el apartado anterior se aplicarán a todo aquel o aquella que interactúe con el sistema, inclusive al personal en labores de administración, mantenimiento y soporte de los sistemas de información, o de inspección de los sistemas, así como a las actuaciones automatizadas y al personal de los centros de atención y soporte a usuarios y usuarias de las administraciones públicas.

3. Requerirá autorización previa del letrado o letrada de la Administración de Justicia competente, o en su caso del superior funcional del servicio, todo acceso que se lleve a cabo a los sistemas de información ya sea a las finalidades del apartado anterior, o a cualquier otra finalidad extraña o ajena o distinta del acceso ordinario que realizan los jueces y juezas, magistrados y magistradas, fiscales, letrados y letradas de la Administración de Justicia, y personal de la oficina judicial a los fines del ejercicio de la actividad jurisdiccional y de la tramitación de los procedimientos judiciales, y del que de conformidad con el presente real decreto-ley y las leyes procesales, realicen las partes, los que hayan justificado interés legítimo y directo, y los y las profesionales jurídicos en el ejercicio de la defensa técnica o de la representación procesal.

4. Cualquier acceso a los sistemas de información por los órganos competentes dependientes del Consejo General del Poder Judicial, de la Fiscalía General del Estado y del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, requerirá la puesta en conocimiento de la Administración prestacional del servicio, que deberá facilitar el acceso para el cumplimiento de las funciones de inspección y control establecidas en las leyes y su normativa de desarrollo.

Artículo 32. *Actuaciones por medios electrónicos.*

1. La presentación de escritos y documentos, los actos de comunicación, la consulta de expedientes judiciales o de su estado de tramitación, cualesquiera otras actuaciones y todos los servicios prestados por la Administración de Justicia se llevarán a cabo por medios electrónicos. Se exceptúa de lo anterior a las personas físicas que, conforme a las leyes procesales, no actúen representadas por Procurador. En estos casos, las personas físicas podrán elegir, en todo momento, si se comunican con la Administración de Justicia a través de medios electrónicos o no, salvo en aquellos supuestos en los que expresamente estén obligadas a relacionarse a través de tales medios.

2. Igualmente se realizarán por medios electrónicos las comunicaciones, traslado de expedientes judiciales electrónicos, documentos y datos, y todo intercambio de información, entre órganos y oficinas judiciales y fiscales, y demás órganos, administraciones e instituciones en el ámbito de la Administración de Justicia, de apoyo o de colaboración con la misma.

Artículo 33. *Inicio del procedimiento por medios electrónicos.*

1. El inicio por los ciudadanos y ciudadanas de un procedimiento judicial por medios electrónicos en aquellos asuntos en los que no sea precisa la representación procesal ni la asistencia letrada, requerirá la puesta a disposición de los interesados, en la sede judicial electrónica, de los correspondientes modelos o impresos normalizados, que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales.

2. En todo caso, cuando los escritos fueran presentados en papel por las personas a las que se refiere el apartado 1 del presente artículo, se procederá a su digitalización por la sección correspondiente del servicio común procesal que tenga atribuidas dichas funciones.

3. Los y las profesionales que se relacionan con la Administración de Justicia presentarán sus demandas y otros escritos por vía telemática, empleando para el escrito principal la firma electrónica establecida en este real decreto-ley.

4. Todo escrito iniciador del procedimiento deberá ir acompañado de un formulario normalizado debidamente cumplimentado en los términos que se establezcan por el Comité técnico estatal de la Administración judicial electrónica.

Artículo 34. *Tramitación del procedimiento utilizando medios electrónicos.*

1. La gestión electrónica de los procedimientos judiciales respetará el cumplimiento de los requisitos formales y materiales establecidos en las normas procesales.

2. Las aplicaciones y sistemas de información utilizados para la gestión por medios electrónicos de los procedimientos deberán garantizar el control de los tiempos y plazos, la identificación del órgano u oficina responsable de los procedimientos, la tramitación ordenada de los expedientes, y asimismo facilitarán la simplificación y la publicidad de los procedimientos.

3. Los sistemas de comunicación utilizados en la gestión electrónica de los procedimientos para las comunicaciones entre las unidades intervinientes en la tramitación de las distintas fases del proceso deberán cumplir los requisitos establecidos en este real decreto-ley y en las disposiciones reglamentarias de desarrollo.

4. Cuando se utilicen medios electrónicos en la gestión del procedimiento, los actos de comunicación y notificación que hayan de practicarse se realizarán conforme a las disposiciones contenidas en este real decreto-ley.

5. La remisión de expedientes administrativos por las distintas administraciones y organismos públicos, prevista en las leyes procesales, se realizará a través de las herramientas de remisión telemática de expedientes administrativos puestas a su disposición.

CAPÍTULO II

Tramitación orientada al dato

Artículo 35. *Principio general de orientación al dato.*

1. Todos los sistemas de información y comunicación que se utilicen en el ámbito de la Administración de Justicia, incluso para finalidades de apoyo a las de carácter gubernativo, asegurarán la entrada, incorporación y tratamiento de la información en forma de metadatos, conforme a esquemas comunes, y en modelos de datos comunes e interoperables que posibiliten, simplifiquen y favorezcan los siguientes fines:

a) La interoperabilidad de los sistemas informáticos a disposición de la Administración de Justicia.
b) La tramitación electrónica de procedimientos judiciales.
c) La búsqueda y análisis de datos y documentos para fines jurisdiccionales y organizativos.
d) La búsqueda y análisis de datos para fines de estadística.
e) La anonimización y seudonimización de datos y documentos.
f) El uso de datos a través de cuadros de mandos o herramientas similares, por cada Administración Pública en el marco de sus competencias.
g) La gestión de documentos.
h) La autodocumentación y la transformación de los documentos.
i) La publicación de información en portales de datos abiertos.
j) La producción de actuaciones judiciales y procesales automatizadas, asistidas y proactivas, de conformidad con la ley.
k) La aplicación de técnicas de inteligencia artificial para los fines anteriores u otros que sirvan de apoyo a la función jurisdiccional, a la tramitación, en su caso, de procedimientos judiciales, y a la definición y ejecución de políticas públicas relativas a la Administración de Justicia.
l) La transmisión de datos entre órganos judiciales, administraciones públicas y asimismo con los ciudadanos y ciudadanas o personas jurídicas, de acuerdo con la ley.
m) Cualquier otra finalidad legítima de interés para la Administración de Justicia.

2. El uso de modelos de datos será obligatorio en las condiciones que se determinen por vía reglamentaria, previo informe del Comité técnico estatal de la Administración judicial electrónica, para el ámbito de todo el territorio del Estado.

Artículo 36. *Intercambios orientados al dato.*

1. Los sistemas informáticos y de comunicación utilizados en la Administración de Justicia posibilitarán el intercambio de información entre órganos judiciales, así como con las partes o interesados, en formato de datos estructurados.
2. La transmisión de información en modelos y estándares de datos entre órganos, oficinas judiciales y oficinas fiscales y entre estos y otros intervinientes se efectuará en los términos que se determinen en la normativa técnica de aplicación, definida por el Comité técnico estatal de la Administración judicial electrónica que en todo caso asegurarán su confiabilidad, su posible automatización y la integración en el expediente judicial electrónico para su visualización por el usuario.
3. A tal efecto, el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes pondrá a disposición para la Administración que lo requiera una plataforma de interoperabilidad de datos, de cuyo funcionamiento y gestión será responsable.
4. Las Administraciones Públicas con competencias en materia de Administración de Justicia puedan intercambiar información y utilizar la información intercambiada a través de dicha plataforma, cumpliendo la normativa técnica que se establezca.

5. Las administraciones públicas con competencia en Justicia impulsarán los intercambios previstos en el apartado anterior con fines de agilización de procesos judiciales y de eficiencia procesal, desarrollando las actuaciones oportunas, entre las que podrá estar la suscripción de convenios con entidades de derecho público o sujetos de derecho privado.

6. En el marco del Comité técnico estatal de la Administración judicial electrónica se favorecerá la colaboración con otras administraciones públicas en la identificación de utilidades para el intercambio de información en formato de datos estructurados, así como en la definición de los parámetros y requisitos de compatibilidad necesarios para ello.

7. La plataforma de interoperabilidad de datos a la que se refiere el apartado 3 deberá ser plenamente interoperable con la Plataforma de Intermediación de Datos de la Administración General del Estado, cuando los datos sean necesarios para la tramitación de alguna administración.

Artículo 37. *Intercambios masivos.*

1. La Administración de Justicia dispondrá de sistemas de intercambio masivo de información.

2. Los sistemas previstos en el apartado anterior podrán estar sujetos a condiciones especiales de servicio, incluso horarias, a fin de evitar la saturación de sistemas o por otras razones de eficiencia tecnológica, dentro de los términos que se definan en el Comité técnico estatal de la Administración judicial electrónica.

Las personas jurídicas, las entidades sin personalidad jurídica a las que la ley reconozca capacidad para ser parte y los colectivos de personas físicas, así como los y las profesionales de la Abogacía, Procura y Graduados y Graduadas Sociales, estarán obligados al uso de los sistemas a los que se refiere el apartado anterior en los casos y condiciones que se establezcan reglamentariamente o por normativa técnica.

3. El uso de los modelos y sistemas de presentación masiva será voluntario en el caso de personas físicas.

Artículo 38. *Documentos generados y presentados de forma automatizada.*

Los escritos y documentos iniciadores o de trámite presentados de forma automatizada deberán cumplir los requisitos procesales, así como los requisitos técnicos que se determinen por normativa de esa naturaleza.

CAPÍTULO III

Del documento judicial electrónico

Artículo 39. *Los documentos judiciales electrónicos.*

1. Tendrá la consideración de documento judicial electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico, según un formato determinado y susceptible de identificación y tratamiento diferenciado admitido en el Esquema Judicial de Interoperabilidad y Seguridad y en las normas que lo desarrollan, y que haya sido generada, recibida o incorporada al expediente judicial electrónico por la Administración de Justicia en el ejercicio de sus funciones, con arreglo a las leyes procesales.

Todos los documentos judiciales electrónicos deberán contener metadatos que posibiliten la interoperabilidad, así como llevar asociado un sello o firma electrónica, en el que quede constancia del órgano emisor, fecha y hora de su presentación o creación, de conformidad con el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, y con la Ley 6/2020, de 11 de noviembre.

2. Tendrá la consideración de documento público el documento judicial electrónico que, además de los requisitos anteriores, incorpore la firma electrónica del letrado o letrada de la Administración de Justicia, siempre que se produzca en el ámbito de las competencias que tuviesen asumidas conforme a las leyes procesales.

Artículo 40. *Documento original y copias electrónicas.*

1. Tendrán la consideración de documento original todos los documentos judiciales electrónicos emanados de los sistemas de gestión procesal y provistos de firma electrónica, así como los correspondientes a los escritos y documentos iniciadores o de trámite presentados por las partes e interesados, una vez hayan sido incorporados al expediente judicial electrónico.

También tendrán la consideración de documentos originales las resoluciones judiciales o administrativas que hubiesen sido firmadas electrónicamente por la autoridad competente para su emisión, a través de cualquiera de los sistemas legalmente establecidos, incluyendo los basados en Código Seguro de Verificación.

No tendrán la consideración de originales, a estos efectos, las copias digitalizadas de otros documentos incorporados al expediente judicial electrónico, salvo que así se declare expresamente.

2. Tendrán la consideración de copias auténticas de documentos judiciales electrónicos originales las emitidas, cualquiera que sea su soporte o cambio de formato que se produzca, bajo la firma del letrado o letrada de la Administración de Justicia, y las que se obtengan mediante actuaciones automatizadas siempre que estén provistas de sello electrónico y concurran además estos requisitos:

a) Que el documento electrónico original se encuentre en el expediente judicial electrónico.

b) Que la información de firma electrónica, y en su caso de sello electrónico cualificado, así como de su contenido, permitan comprobar la coincidencia con dicho documento.

3. Las copias previstas en el apartado anterior gozarán de la eficacia prevista en las leyes procesales, siempre que la información de firma electrónica y, en su caso, de marca de tiempo o sello electrónico cualificado, así como de su contenido, permitan comprobar la coincidencia con dicho documento.

4. También serán copias auténticas, siempre que se emitan bajo la firma del letrado o letrada de la Administración de Justicia:

a) Los documentos electrónicos generados por la oficina judicial, de acuerdo con la normativa técnica del Comité técnico estatal de la Administración judicial electrónica, sobre documentos judiciales en soporte papel que consten en los archivos judiciales.

b) La digitalización de los documentos en papel presentados por quienes no estén obligados a relacionarse con la Administración de Justicia por medios electrónicos, siempre que se realice en los términos definidos por el Comité técnico estatal de la Administración judicial electrónica, que en todo caso, garantizarán su autenticidad, integridad y la constancia de la identidad con el documento imagen, así como los establecidos en los sistemas de lo que se dejará constancia, pudiendo impugnarse su validez por los cauces procesales procedentes.

5. Las copias auténticas se expedirán siempre a partir de un original o de otra copia auténtica, y tendrán la misma validez y eficacia que los documentos originales. Esta obtención podrá hacerse de forma automatizada mediante el correspondiente sello electrónico, y, en caso de que se alterase el formato original, deberá incluirse en los metadatos la condición de copia.

6. Se podrá verificar la autenticidad e integridad de todos los documentos judiciales electrónicos, preferiblemente por medios criptográficos automatizados, siendo válidos también los sistemas basados en Código Seguro de Verificación que permitan comprobar la autenticidad de la copia mediante el acceso a los archivos electrónicos de la oficina judicial emisora. A través de las sedes judiciales electrónicas se harán públicas las direcciones de comprobación de los códigos de tales documentos.

7. No se permitirá la impresión ni expedición de documentos en formato papel, salvo cuando el letrado o letrada de la Administración de Justicia, en atención a las circunstancias concurrentes, acuerde su expedición, o se solicite por quien no venga obligado a relacionarse con la Administración de Justicia por medios electrónicos. En estos casos, el documento generado tendrá la consideración de original, siempre que contenga el Código Seguro de Verificación, para garantizar su autenticidad e integridad.

Para garantizar la identidad y contenido de las copias electrónicas o en papel, y por tanto su carácter de copias auténticas, se estará a lo previsto en el Esquema Judicial de Interoperabilidad y Seguridad, así como en la normativa técnica de desarrollo.

8. Tendrán la consideración de copias anonimizadas las obtenidas conforme a la normativa técnica definida por el Comité técnico estatal de la Administración judicial electrónica, mediante extractos del contenido del documento origen a través de la utilización de métodos electrónicos automatizados, que permitan mantener la confidencialidad de aquellos datos que se determinen.

CAPÍTULO IV

La presentación de documentos

Artículo 41. *Forma de presentación de documentos.*

1. Las partes o intervinientes deberán presentar todo tipo de documentos y actuaciones para su incorporación al expediente judicial electrónico en formato electrónico.

Se exceptúan de lo dispuesto en el párrafo anterior aquellos casos previstos en las leyes.

2. La presentación de los documentos en los procedimientos judiciales se ajustará a lo establecido en las leyes procesales, garantizándose en todo caso la obtención de recibo de su presentación, donde quede constancia de su contenido, fecha y hora. La presentación de estos documentos se realizará electrónicamente a través de los sistemas destinados a tal fin, pudiendo éstos incluir sistemas automatizados de presentación.

3. Cuando el documento se presente en un formato distinto al electrónico, se procederá de acuerdo con lo previsto en este real decreto-ley.

Artículo 42. *Presentación de documentos por medios electrónicos.*

1. La presentación de escritos y documentos, o cualesquiera otros medios o instrumentos, por medios electrónicos, incluso los que sean generados de forma automatizada, habrá de cumplir con lo dispuesto en las leyes procesales y con la normativa técnica establecida en el marco del Comité técnico estatal de la Administración judicial electrónica en las leyes procesales y, en su caso, en la normativa técnica. Deberán constar necesariamente:

a) La identidad de la persona que lo presente.
b) El órgano judicial, la oficina judicial u oficina fiscal a los que va dirigido.
c) El tipo y número de procedimiento al que se debe incorporar.
d) La fecha de presentación.

2. Los documentos que se hubiesen presentado electrónicamente deberán conservarse en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. La eliminación de dichos documentos deberá ser autorizada de acuerdo con lo dispuesto en la normativa aplicable sobre archivos judiciales.

3. Cuando se planteen dudas sobre la integridad de los documentos, a incluir o ya incluidos en el expediente judicial electrónico, o existan dudas derivadas de la calidad de la copia, la oficina judicial podrá requerir al presentante para que exhiba el documento o la información original, con el fin de proceder a su examen y evaluar la procedencia de incorporación al expediente judicial electrónico. En caso de impugnación, se procederá conforme a lo dispuesto en las leyes procesales.

Artículo 43. *Presentación de documentos en papel o en otros soportes no digitales.*

1. Los documentos en papel que se aporten en cualquier momento del procedimiento, siempre que la parte que los presente no venga obligada a relacionarse electrónicamente

con la Administración de Justicia, se deberán digitalizar por la oficina judicial e incorporar al expediente judicial electrónico.

La digitalización a la que se refiere el apartado anterior habrá de cumplir con la normativa técnica establecida en el marco del Comité técnico estatal de la Administración judicial electrónica, y con lo dispuesto en el presente real decreto-ley, las leyes procesales u otras normas de desarrollo.

2. Todos aquellos documentos que se encuentren en formatos distintos del papel deberán ser aportados por quien los presente en formato compatible para su incorporación al expediente judicial electrónico.

Si la persona que los presenta no está obligada a relacionarse con la Administración de Justicia por medios electrónicos, se procederá a su digitalización con los medios puestos a disposición de la oficina judicial o fiscal por la Administración competente.

3. En caso de que el documento no pueda digitalizarse debido a razones históricas, de protección del patrimonio u otras razones, o cuando su conservación así lo aconseje a juicio del letrado o letrada de la Administración de Justicia, se presentará en el formato original y se conservará por la oficina judicial en la forma que establezca la ley.

4. La persona interesada deberá hacer llegar dicha documentación al órgano judicial, la oficina judicial u oficina fiscal en la forma que establezcan las normas procesales, y deberá hacer referencia a los datos identificativos del envío electrónico al que no pudo ser adjuntado, presentando el original ante el órgano judicial en el día hábil siguiente a aquel en que se hubiera efectuado el envío electrónico del escrito, que deberá acompañar en todo caso. Si no se presentara en este plazo, el documento se tendrá por no presentado a todos los efectos.

5. Se dejará constancia en el expediente judicial electrónico, por diligencia del letrado o letrada de la Administración de Justicia, de la existencia de documentos en formato no electrónico.

6. Las administraciones públicas con competencias sobre medios materiales en la Administración de Justicia proveerán a las oficinas judiciales y oficinas fiscales de los medios necesarios para la conversión de estos documentos.

7. Los documentos presentados que no deban ser conservados serán devueltos a la persona que los hubiere presentado inmediatamente después de su digitalización. En caso de imposibilidad, se les dará el destino previsto en la normativa correspondiente sobre archivos judiciales, todo ello sin perjuicio de la previsión derivada del artículo 82.1 del presente real decreto-ley.

Artículo 44. *Presentación y traslado de copias.*

1. El traslado de copias entre profesionales se realizará por vía telemática de forma simultánea a la presentación telemática de escritos y documentos originales ante el tribunal, oficina judicial u oficina fiscal correspondiente.

2. Las copias que por disposición legal deban trasladarse a las partes se presentarán en formato digital, debiendo procederse conforme a lo previsto en este real decreto-ley en caso de que su destinatario no esté obligado a comunicarse por medios electrónicos con la Administración de Justicia.

3. Para ello, los y las profesionales podrán servirse de códigos de almacenamiento que garanticen la identidad, integridad e invariabilidad del contenido, lo cual será responsabilidad del profesional que lo presente.

Artículo 45. *Aportación de documentos en las actuaciones orales telemáticas.*

1. En las actuaciones realizadas con intervención telemática de uno o varios intervinientes, y en los actos y servicios no presenciales, las partes podrán presentar y visualizar la documentación con independencia de si su intervención se realiza por vía telemática o presencial. A tal fin, los intervinientes por vía telemática que quieran presentar documentación en el mismo acto deberán presentarla por la misma vía, incluso en los casos en los que por regla general no estén obligados a relacionarse con la Administración de Justicia por medios electrónicos, y siempre de conformidad con las normas procesales.

2. Los documentos que puedan o deban ser aportados en el momento del juicio o actuación de que se trate, se presentarán de conformidad con lo establecido en este real

decreto-ley y con la normativa del Comité técnico estatal de la Administración judicial electrónica.

3. Cuando la parte que presente el documento o prueba no pudiese remitir la documentación en la forma prevista anteriormente, deberá justificar la circunstancia que impida su remisión, así como ponerlo en conocimiento del órgano judicial de manera previa a la vista o actuación, a fin de que por éste se disponga lo que proceda.

Artículo 46. *Acceso a la información sobre el estado de tramitación.*

1. Los servicios electrónicos que faciliten a las partes y a los y las profesionales que intervienen ante la Administración de Justicia el acceso al estado de tramitación del procedimiento o la consulta del expediente judicial electrónico, garantizarán la aplicación de la normativa que pueda establecer restricciones a dicha información, con pleno respeto a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; en la Ley Orgánica 3/2018, de 5 de diciembre; en la Ley Orgánica 7/2021, de 26 de mayo, y su normativa de desarrollo, con las especialidades establecidas en la Ley Orgánica 6/1985, de 1 de julio, y en las leyes procesales.

2. La información sobre el estado de tramitación del procedimiento comprenderá la relación de los actos de trámite realizados, con indicación sobre su contenido, así como la fecha en la que fueron dictadas las resoluciones.

CAPÍTULO V

Del expediente judicial electrónico

Artículo 47. *Expediente judicial electrónico.*

1. El expediente judicial electrónico es el conjunto ordenado de datos, documentos, trámites y actuaciones electrónicas, así como de grabaciones audiovisuales, correspondientes a un procedimiento judicial, cualquiera que sea el tipo de información que contengan y el formato en el que se hayan generado.

2. Se asignará un número de identificación general a cada expediente judicial electrónico, que será único e inalterable a lo largo de todo el proceso, permitiendo su identificación unívoca por cualquier tribunal u oficina del ámbito judicial en un entorno de intercambio de datos.

3. Todo expediente judicial electrónico tendrá un índice electrónico, firmado por la oficina judicial actuante o por procesos automatizados conforme a lo previsto en este real decreto-ley. Este índice garantizará la integridad del expediente judicial electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes judiciales electrónicos.

4. La remisión de expedientes se sustituirá a todos los efectos legales por la puesta a disposición del expediente judicial electrónico, pudiendo obtener copia electrónica del mismo todos aquellos que tengan derecho conforme a lo dispuesto en las normas procesales.

5. La puesta a disposición de los documentos judiciales electrónicos se realizará en la forma establecida en el presente real decreto-ley para el acceso y puesta a disposición del expediente judicial electrónico.

Artículo 48. *Sistema Común de Intercambio de documentos y expedientes judiciales electrónicos.*

1. El Sistema Común de Intercambio de documentos y expedientes judiciales electrónicos tendrá por objeto posibilitar la itineración de expedientes electrónicos y la transmisión de documentos electrónicos de una oficina u órgano judicial o fiscal a otro, en los casos en los que corresponda por aplicación de las leyes procesales, e independientemente de que los tribunales u oficinas implicados utilicen el mismo o distintos sistemas de gestión procesal, y estará bajo la responsabilidad y gestión del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes.

2. Las Administraciones Públicas con competencias en materias de Administración de Justicia asegurarán la interoperabilidad de los sistemas de gestión procesal con el Sistema Común de Intercambio de documentos y expedientes.

3. Se establecerán sus condiciones de funcionamiento con ámbito en todo el territorio del Estado, así como los requisitos técnicos y previsiones para la interoperabilidad de los sistemas de Justicia con el mismo, por el Comité técnico estatal de la Administración judicial electrónica.

CAPÍTULO VI

De las comunicaciones electrónicas

Artículo 49. *Comunicaciones electrónicas en el ámbito de la Administración de Justicia.*

1. Las comunicaciones en el ámbito de la Administración de Justicia se practicarán por medios electrónicos, inclusive los actos procesales de comunicación previstos en el artículo 149 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

2. Los órganos, oficinas judiciales u oficinas fiscales llevarán a cabo las comunicaciones por otros medios cuando las personas no obligadas a relacionarse con la Administración de Justicia por medios electrónicos no elijan hacer uso de estos medios.

3. Aquellas personas que no estén obligadas a relacionarse con la Administración de Justicia por medios electrónicos podrán elegir, en cualquier momento, la manera de comunicarse con la Administración de Justicia, y que las comunicaciones sucesivas se practiquen o dejen de practicarse por medios electrónicos.

4. La persona interesada podrá identificar un dispositivo electrónico y, en su caso, una dirección de correo electrónico que servirán para el envío de información y de avisos de puesta a disposición de actos de comunicación.

5. Las comunicaciones a través de medios electrónicos se realizarán, en todo caso, con sujeción a lo dispuesto en la legislación procesal y serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas y del contenido íntegro de las comunicaciones, y que se identifique al remitente y al destinatario de las mismas. La acreditación de la práctica del acto de comunicación se incorporará al expediente judicial electrónico.

Artículo 50. *Actos procesales de comunicación por medios electrónicos. Excepciones.*

1. Los actos procesales de comunicación previstos en el artículo 149 de la Ley de Enjuiciamiento Civil que se lleven a cabo por medios electrónicos se podrán practicar mediante comparecencia en la Carpeta Justicia o correspondiente sede judicial electrónica, a través de la dirección electrónica habilitada única prevista en la Ley 39/2015, de 1 de octubre, o por otros medios electrónicos que se establezcan reglamentariamente y garanticen el ejercicio de las facultades y derechos previstos en este real decreto-ley. Ello sin perjuicio de la eficacia de la comunicación cuando el destinatario se dé por enterado, conforme a lo dispuesto en el artículo 166.2 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Se entenderá por comparecencia en la Carpeta Justicia o en la sede judicial electrónica el acceso por la persona interesada o su representante debidamente identificado al contenido del acto de comunicación.

2. En caso de que el acto de comunicación no pueda llevarse a cabo por medios electrónicos, se procederá a su práctica en las demás formas establecidas en las leyes procesales, e incorporándose al expediente judicial electrónico la información acreditativa de la práctica del acto de comunicación.

3. Todos los actos de comunicación en papel que se deban practicar a la persona interesada que no esté obligada a relacionarse telemáticamente con la Administración de Justicia, deberán ser puestos a su disposición en la Carpeta Justicia, y en su caso en la correspondiente sede judicial electrónica, para que pueda acceder a su contenido de forma voluntaria y con plenos efectos.

Artículo 51. *Punto Común de Actos de Comunicación.*

1. Las administraciones competentes en materia de justicia garantizarán la existencia de un Punto Común de Actos de Comunicación, en el que los y las profesionales puedan acceder a todos los actos de comunicación de los que sean destinatarios, cualquiera que sea órgano judicial, oficina judicial u oficina fiscal que los haya emitido.

2. El Punto Común de Actos de Comunicación interoperará en tiempo real y de manera automática con los sistemas de gestión procesal. Además, permitirá a los órganos judiciales acceder a todos los actos de comunicación electrónicos que desde dichos sistemas se practiquen a las partes e interesados.

3. Asimismo, el Punto Común de Actos de Comunicación interoperará con el sistema de intercambio de registros de la Administración Pública con el objeto de canalizar las comunicaciones entre los órganos de la Administración General del Estado y los órganos judiciales, oficinas judiciales y oficinas fiscales. Las Administraciones Públicas con competencias en materias de Administración de Justicia definirán el tipo de comunicaciones o avisos de comunicación que podrán ser remitidos a través de sistema de intercambio de registros de la Administración Pública, pudiendo mantener la sede judicial electrónica cómo punto preferente de acceso a la notificación.

Artículo 52. *Comunicaciones masivas.*

Las comunicaciones y actos de comunicación por vía electrónica podrán realizarse individualmente o de forma masiva, en los términos que se definan por el Comité técnico estatal de la Administración judicial electrónica. En este caso deberá tenerse en cuenta lo establecido en el artículo 37 del presente real decreto-ley.

Artículo 53. *Comunicaciones orientadas al dato.*

Los canales electrónicos utilizados para la realización de comunicaciones unidireccionales o bidireccionales estarán metadatados y orientados al dato, y asegurarán la entrada, incorporación y tratamiento de la información en forma de metadatos conforme a esquemas comunes, y en modelos de datos comunes e interoperables, a los fines previstos en el artículo 49 de este real decreto-ley.

Artículo 54. *Comunicación edictal electrónica.*

1. La publicación de resoluciones y actos de comunicación que por disposición legal deban fijarse en tablón de anuncios, así como la publicación de los actos de comunicación procesal que deban ser objeto de inserción en el «Boletín Oficial del Estado» o en el Boletín o Diario Oficial de la Comunidad Autónoma o de la provincia respectiva, serán sustituidas en todos los órdenes jurisdiccionales por su publicación en el Tablón Edictal Judicial Único previsto en el artículo 236 de la Ley Orgánica 6/1985, de 1 de julio.

En todo caso, el destinatario o destinataria del acto de comunicación edictal podrá obtener copia íntegra de la resolución objeto de la comunicación edictal mediante acceso a la sede judicial electrónica, previa identificación por alguno de los medios previstos en este real decreto-ley, todo ello sin perjuicio de las restricciones que pudiera establecer la normativa en materia de protección de datos.

2. El Tablón Edictal Judicial Único será publicado electrónicamente por la Agencia Estatal Boletín Oficial del Estado, en la forma que se disponga reglamentariamente impidiendo en todo caso la indexación por motores de búsqueda. A tal efecto, la Agencia Estatal Boletín Oficial del Estado pondrá a disposición de los órganos judiciales un sistema automatizado de remisión y gestión telemática que garantizará la celeridad en la publicación de los edictos, su correcta y fiel inserción, así como la identificación del órgano remitente.

3. Las publicaciones que, en cumplimiento de lo previsto en las leyes procesales, deban hacerse en el Tablón Edictal Judicial Único serán gratuitas en todo caso, sin que proceda contraprestación económica por parte de quienes las hayan solicitado. Igualmente serán gratuitas las consultas en el tablón, así como las suscripciones que los ciudadanos y ciudadanas puedan realizar a su sistema de alertas.

Artículo 55. *Comunicaciones transfronterizas.*

El Ministerio de la Presidencia, Justicia y Relaciones con las Cortes establecerá un servicio o aplicación común como nodo para las comunicaciones electrónicas transfronterizas relativas a actuaciones de cooperación jurídica internacional. Deberá cumplir los requisitos de interoperabilidad que se hayan convenido en el marco de la Unión Europea o, en su caso, de la normativa convencional de aplicación, y permitir el cumplimiento de las normas sustantivas y procesales de la Unión Europea y de los Tratados o Acuerdos internacionales en vigor.

Las Comunidades Autónomas con competencia en medios personales y materiales de la Administración de Justicia asegurarán la interoperabilidad de los sistemas que establezcan con el servicio o aplicación común previsto en este artículo.

CAPÍTULO VII

De las actuaciones automatizadas, proactivas y asistidas

Artículo 56. *Actuaciones automatizadas.*

1. Se entiende por actuación automatizada la actuación procesal producida por un sistema de información adecuadamente programado sin necesidad de intervención humana en cada caso singular.

2. Los sistemas informáticos utilizados en la Administración de Justicia posibilitarán la automatización de las actuaciones de trámite o resolutorias simples, que no requieren interpretación jurídica. Entre otras:

a) El numerado o paginado de los expedientes.
b) La remisión de asuntos al archivo cuando se den las condiciones procesales para ello.
c) La generación de copias y certificados.
d) La generación de libros.
e) La comprobación de representaciones.
f) La declaración de firmeza, de acuerdo con la ley procesal.

3. Se entiende por actuaciones proactivas las actuaciones automatizadas, auto-iniciadas por los sistemas de información sin intervención humana, que aprovechan la información incorporada en un expediente o procedimiento de una Administración Pública con un fin determinado, para generar avisos o efectos directos a otros fines distintos, en el mismo o en otros expedientes, de la misma o de otra Administración Pública, en todo caso conformes con la ley.

En el marco del Comité técnico estatal de la Administración judicial electrónica se favorecerá la colaboración con otras administraciones públicas en la identificación de actuaciones que, en su caso, puedan ser proactivos, así como en la definición de los parámetros y requisitos de compatibilidad necesarios para ello.

4. Con relación a las actuaciones previstas en este artículo, los sistemas de la Administración de Justicia asegurarán:

a) Que todas las actuaciones automatizadas y proactivas se puedan identificar como tales, trazar y justificar.
b) Que sea posible efectuar las mismas actuaciones en forma no automatizada.
c) Que sea posible deshabilitar, revertir o dejar sin efecto las actuaciones automatizadas ya producidas.

Artículo 57. *Actuaciones asistidas.*

1. Se considera actuación asistida aquella para la que el sistema de información de la Administración de Justicia genera un borrador total o parcial de documento complejo basado en datos, que puede ser producido por algoritmos, y puede constituir fundamento o apoyo de una resolución judicial o procesal.

2. En ningún caso el borrador documental así generado constituirá por sí una resolución judicial o procesal, sin validación de la autoridad competente. Los sistemas de la

Administración de Justicia asegurarán que el borrador documental sólo se genere a voluntad del usuario y pueda ser libre y enteramente modificado por éste.

3. La constitución de resolución judicial o procesal requerirá siempre la validación del texto definitivo, por el juez o jueza, magistrado o magistrada, fiscal o letrado o letrada de la Administración de Justicia, en el ámbito de sus respectivas competencias y bajo su responsabilidad, así como la identificación, autenticación o firma electrónica que en cada caso prevea la ley, además de los requisitos que las leyes procesales establezcan.

Artículo 58. *Requisitos comunes de las actuaciones automatizadas, proactivas y asistidas.*

1. En caso de actuación automatizada, asistida o proactiva podrá realizarse por el Comité técnico estatal de la Administración judicial electrónica la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, la auditoría del sistema de información y de su código fuente.

2. Los criterios de decisión serán públicos y objetivos, dejando constancia de las decisiones tomadas en cada momento.

3. Los sistemas incluirán los indicadores de gestión que se establezcan por la Comisión Nacional de Estadística Judicial y el Comité técnico estatal de la Administración judicial electrónica, cada uno en el ámbito de sus competencias.

TÍTULO IV

De los actos y servicios no presenciales

CAPÍTULO I

Actuaciones judiciales y actos y servicios no presenciales

Artículo 59. *Atención y servicios no presenciales.*

1. La atención a los ciudadanos y ciudadanas se realizará, mediante presencia telemática, por videoconferencia u otro sistema similar, siempre que el ciudadano o ciudadana así lo interese y sea posible en función de la naturaleza del acto o información requerida y con cumplimiento de la normativa aplicable en materia de protección de datos de carácter personal.

2. La atención a los y las profesionales podrá también realizarse por presencia telemática o videoconferencia, siempre de conformidad con estos.

3. La atención al público y a los y las profesionales por videoconferencia o sistema similar requerirá la participación del ciudadano, ciudadana o profesional desde un punto de acceso seguro.

4. El personal al servicio de la Administración de Justicia deberá gestionar las citas para la atención telemática a través de un sistema que otorgue seguridad jurídica al proceso de atención y garantice la encriptación e integridad de las comunicaciones.

5. Las administraciones con competencias en Justicia garantizarán la interoperabilidad y compatibilidad de los distintos sistemas que posibiliten la presencia telemática y la videoconferencia que se utilicen en cada uno de los ámbitos territoriales de prestación del servicio público de Justicia.

Artículo 60. *Regla general de identificación y firma.*

1. Sin perjuicio de la identificación electrónica regulada en los artículos siguientes y de la aplicación de las normas contenidas en leyes procesales, las personas intervinientes en una videoconferencia deberán identificarse al inicio del acto.

El juez o jueza, magistrado o magistrada, representante del Ministerio fiscal o letrado o letrada de la Administración de Justicia que dirija el acto o actuación adoptará las disposiciones oportunas a tal fin.

Cuando la actuación no sea dirigida por los anteriores, el funcionario público que provea el servicio asegurará que los intervinientes se identifiquen al inicio.

2. Asimismo, el acceso de ciudadanos, ciudadanas y los y las profesionales a aquellas actuaciones judiciales y procesales celebradas por videoconferencia en las que sean parte o tengan un interés legítimo y directo, se realizará preferentemente mediante identificación electrónica, que será previa o simultánea al momento de cada actuación y específica para la misma.

3. Lo dispuesto en los anteriores apartados podrá exceptuarse en el caso de testigos o peritos protegidos, agentes de policía, agentes de policía encubiertos, y, en definitiva, en el de toda aquella persona cuya identidad haya de ser preservada en el proceso de acuerdo con la ley.

4. La oficina judicial o fiscal comprobará la identidad de las personas intervinientes en las actuaciones realizadas por procedimientos electrónicos a través de los datos básicos de identificación que hayan sido aportados previamente por ellas, conforme a lo establecido en el presente artículo.

5. En la intervención por videoconferencia no podrán emplearse sistemas o aplicaciones que alteren o distorsionen la imagen y el sonido transmitido, salvo excepciones relativas a la salvaguarda de la identidad en los casos previstos en el apartado 3 de este artículo.

6. Los intervinientes en una videoconferencia deberán observar las mismas normas de decoro, vestimenta y respeto exigidas en las actuaciones realizadas presencialmente en las salas de vistas y en las sedes de los tribunales, oficinas judiciales y oficinas fiscales.

7. Cuando una actuación realizada por videoconferencia exija la firma de la persona interviniente por este mismo medio, requerirá, de manera general:

a) La verificación previa de la información a firmar por parte de la persona interviniente.

b) La autenticación de la persona interviniente de conformidad con lo establecido en este real decreto-ley.

El uso de las firmas en cada una de las actuaciones realizadas por videoconferencia se determinará en el marco del Comité técnico estatal de la Administración judicial electrónica.

Artículo 61. *Efectos de las actuaciones por videoconferencia.*

1. El incumplimiento de lo establecido en los artículos anteriores no priva por sí solo de efectos procesales y jurídicos a la actuación llevada a cabo por videoconferencia, ni supone la ineficacia o nulidad de la misma.

2. Si, una vez celebrada la actuación correspondiente, se impugnare la identificación o la firma realizada en la videoconferencia, se procederá por la Administración competente a comprobar que la misma cumple todos los requisitos y condiciones establecidos en el artículo anterior.

3. Si dichas comprobaciones ofrecen un resultado positivo, se presumirá la autenticidad de la identificación, siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación.

4. Si las comprobaciones ofrecen resultado negativo o si, a pesar de su resultado positivo, el impugnante sostuviere la impugnación, el juez o Tribunal competente en el asunto resolverá motivadamente lo que corresponda, previa audiencia de las partes.

Artículo 62. *Puntos de acceso seguros y lugares seguros.*

1. A los efectos de las normas sobre atención al público y a los y las profesionales mediante presencia telemática contenidas en este real decreto-ley, y de las normas procesales sobre intervención en actos procesales mediante presencia telemática, tendrán la consideración de punto de acceso seguro y de lugar seguro, respectivamente, aquellos que se ajusten a lo previsto en este artículo.

2. Son puntos de acceso seguros los dispositivos y sistemas de información que cumplan los requisitos que se determinen por la normativa del Comité técnico estatal de la Administración judicial electrónica, que en todo caso deberán reunir, al menos, los siguientes:

a) Permitir la transmisión segura de las comunicaciones y la protección de la información.

b) Permitir y garantizar la identificación de los intervinientes.

c) Cumplir los requisitos de integridad, interoperabilidad, confidencialidad y disponibilidad de lo actuado.

3. Son lugares seguros aquellos que cumplan los requisitos que se determinen por la normativa del Comité técnico estatal de la Administración judicial electrónica, que en todo caso deberán reunir, al menos, los siguientes:

a) Disponer de dispositivos y sistemas que tengan la condición de punto de acceso seguro, conforme al apartado anterior.
b) Garantizar la comprobación de la identidad de los intervinientes y la autonomía de su intervención.
c) Asegurar todas las garantías del derecho de defensa, inclusive la facultad de entrevistarse reservadamente con el Abogado o Abogada.
d) Disponer de medios que permitan la digitalización de documentos para su visualización por videoconferencia.

4. Además, se entenderán por lugares seguros en todo caso:

a) La oficina judicial correspondiente al tribunal competente, o cualquier otra oficina judicial o fiscal, y las oficinas de justicia en el municipio.
b) Los Registros Civiles, para actuaciones relacionadas con su ámbito.
c) El Instituto Nacional de Toxicología y Ciencias Forenses y los Institutos de Medicina Legal, para la intervención de los Médicos Forenses, Facultativos, Técnicos y Ayudantes de Laboratorio.
d) Las sedes de las Fuerzas y Cuerpos de Seguridad del Estado, para la intervención de sus miembros.
e) Las sedes oficiales de la Abogacía del Estado, del Servicio Jurídico de la Administración de la Seguridad Social y de los Servicios Jurídicos de las Comunidades Autónomas, para la intervención de los miembros de tales servicios.
f) Los Centros penitenciarios, órganos dependientes de Instituciones Penitenciarias, centros de internamiento de extranjeros y centros de internamiento de menores, para las personas internas y funcionarios públicos.
g) Cualesquiera otros lugares que se establezcan por Reglamento de aplicación en todo el territorio del Estado, previo informe favorable del Comité técnico estatal de la Administración judicial electrónica.

Artículo 63. *Medios técnicos.*

El Ministerio de la Presidencia, Justicia y Relaciones con las Cortes y las Comunidades Autónomas con competencias en materia de Justicia dotarán a las oficinas judiciales y fiscales de los medios técnicos adecuados para que puedan garantizarse las actuaciones y servicios no presenciales.

Artículo 64. *Actuaciones no jurisdiccionales.*

1. Las actuaciones no jurisdiccionales en las que intervengan jueces o juezas, magistrados o magistradas, letrados o letradas de la Administración de Justicia y Ministerio fiscal podrán realizarse de forma presencial o mediante la utilización de videoconferencia, o por cualesquiera otros sistemas que permitan la reproducción del sonido y de la imagen.
2. Las Juntas de jueces y las Salas de Gobierno podrán realizar sus actuaciones de forma telemática, en los términos establecidos en el presente real decreto-ley y de acuerdo con lo que al efecto se disponga reglamentariamente por el Consejo General del Poder Judicial. De la misma forma telemática podrán celebrarse las Juntas de fiscales y de letrados y letradas de la Administración de Justicia.

Artículo 65. *Utilización de las salas de vistas virtuales.*

1. Se considerarán salas de vistas virtuales aquellas generadas en el medio digital, que dispongan de los mismos medios de grabación, seguridad e integración con el expediente judicial electrónico que las salas de vistas presenciales o físicas, pero que no necesiten de

espacios físicos especiales, y permitan su uso de manera independiente al de las salas presenciales.

2. Las administraciones públicas con competencias en materia de Justicia proveerán a jueces y juezas, magistrados y magistradas, fiscales, letrados y letradas de la Administración de Justicia y personal al servicio de la Administración de Justicia de salas virtuales para la realización de aquellas actuaciones que deban llevar a cabo en el ejercicio de sus funciones. Mediante norma reglamentaria se establecerá la forma y requisitos de su uso.

3. La utilización indebida de las salas virtuales podrá ser sancionada, en su caso, en los términos que determine la normativa disciplinaria aplicable.

CAPÍTULO II

La emisión de las actuaciones celebradas por medios electrónicos

Artículo 66. *La emisión de los actos de juicio y vistas electrónicos.*

1. Los actos de juicio, vistas y otras actuaciones que de acuerdo con las leyes procesales se hayan de practicar en audiencia pública, cuando se celebren con participación telemática de todos los intervinientes, se retransmitirán públicamente conforme a los aspectos o especificidades técnicas que se establezcan por el Comité técnico estatal de la Administración judicial electrónica.

Los sistemas de información y comunicación podrán establecer diferentes niveles de seguridad y acceso del público a la retransmisión.

En los casos del artículo 138.2 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil; 681.1 de la Ley de Enjuiciamiento Criminal, o en cualquier otro en el que la ley procesal permita la restricción de la publicidad, el juez o tribunal podrá acordar la no retransmisión en la forma prevista por la ley procesal.

2. En los actos de juicio, vistas y audiencias celebradas con presencia física en la sala de vistas de alguno o algunos de los intervinientes, y en aquellos en los que la publicidad quede garantizada mediante el acceso abierto a la sala de vistas, el juez o tribunal podrá acordar mediante auto la no retransmisión en los casos del apartado 1, párrafo tercero y además cuando lo considerase estrictamente necesario en atención a las circunstancias concurrentes.

3. Asimismo, en el ámbito penal, de acuerdo con el artículo 682 de la Ley de Enjuiciamiento Criminal, el juez o tribunal, previa audiencia de las partes, podrá restringir la presencia de los medios de comunicación audiovisuales en las sesiones del juicio y establecer limitaciones a las grabaciones y toma de imágenes, a la publicidad de informaciones sobre la identidad de las víctimas, de los testigos o peritos o de cualquier otra persona que intervenga en el juicio.

4. En las sedes judiciales electrónicas se publicará el listado de los actos de juicio, vistas y audiencias a celebrar por cada órgano judicial, y la forma de acceso a los mismos a efectos de publicidad.

5. En el caso de las actuaciones orales que se celebren ante el letrado o letrada de la Administración de Justicia se aplicará lo previsto en los apartados anteriores.

Los letrados o letradas de la Administración de Justicia podrán acordar mediante decreto la no retransmisión en los casos previstos en este artículo en materias de su exclusiva competencia.

CAPÍTULO III

Protección de datos de las actuaciones recogidas en soporte audiovisual

Artículo 67. *Control sobre la difusión de actuaciones telemáticas.*

1. Las actuaciones judiciales que se realicen de forma telemática deberán respetar la normativa vigente en materia de protección de datos.

2. En las actuaciones judiciales telemáticas y en los servicios no presenciales descritos en el presente título, las partes, intervinientes o cualesquiera personas que tengan acceso a

dicha actuación, no podrán grabar, tomar imágenes o utilizar cualesquiera medios que permitan una posterior reproducción del sonido y/o de la imagen de lo acontecido.

3. Las grabaciones a las que cualquier persona haya tenido acceso con motivo de un procedimiento judicial no podrán ser utilizadas, sin autorización judicial, para fines distintos de los jurisdiccionales.

4. En caso de incumplimiento de las obligaciones establecidas en el presente artículo, el juez o tribunal podrá imponer motivadamente una multa de 180 a 60.000 euros, que estará sujeta al régimen de recursos previsto en el título V del libro VII de la Ley Orgánica 6/1985, de 1 de julio, sin perjuicio de las sanciones que correspondan si la actuación constituyera una infracción a la normativa sobre protección de datos de carácter personal, y de las responsabilidades administrativas, civiles o penales a que haya lugar. Para la imposición de las sanciones se tendrá en cuenta la intencionalidad, el perjuicio real causado a la Administración o a los ciudadanos y la reiteración o reincidencia de la conducta.

CAPÍTULO IV

Seguridad de los entornos remotos de trabajo

Artículo 68. *Entornos remotos de trabajo.*

1. Se entiende por entornos remotos de trabajo los espacios de trabajo que, cumpliendo los requisitos de seguridad, interoperabilidad y capacidad en la gestión, permitan la prestación del servicio público de Justicia mediante la utilización de las nuevas tecnologías, con independencia de si la prestación del servicio se realiza de forma presencial.

2. Los entornos remotos de trabajo deberán disponer de las medidas de seguridad adecuadas que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de la información gestionada en los mismos, de acuerdo con la normativa que sea de aplicación y siempre que cumplan las condiciones de uso y seguridad que se considere por la administración competente. En concreto, asegurarán la identificación de los usuarios y el control de accesos.

3. El Esquema Nacional de Seguridad y el Esquema Judicial de Interoperabilidad y Seguridad fijarán los requisitos mínimos que todas las administraciones públicas con competencias en materia de Justicia han de garantizar en relación con los entornos remotos de trabajo.

4. Lo dispuesto en este artículo se entiende sin perjuicio de lo establecido en el artículo 62 del presente real decreto-ley en relación a las actuaciones telemáticas en entornos seguros.

TÍTULO V

Los Registros de la Administración de Justicia y los archivos electrónicos

CAPÍTULO I

Del Registro de Datos para el contacto electrónico con la Administración de Justicia

Artículo 69. *Registro de Datos para el contacto electrónico con la Administración de Justicia.*

1. El Registro de Datos de contacto electrónico con la Administración de Justicia incluirá los datos de contacto que los ciudadanos, ciudadanas y profesionales que intervienen ante la Administración de Justicia faciliten a un órgano u oficina judicial, fiscalía u oficina fiscal durante la tramitación de cualquier procedimiento en el que sean partes o interesados, y serán accesibles para todos los órganos y oficinas judiciales, fiscalías y oficinas fiscales con fines jurisdiccionales, de acuerdo con lo dispuesto en la normativa sobre protección de datos de carácter personal que resulte aplicable.

2. Los y las profesionales que intervienen ante la Administración de Justicia están obligados a proporcionar sus datos de carácter personal para que se incluyan en el Registro previsto en el presente artículo.

3. El Registro de Datos de contacto electrónico con la Administración de Justicia dispondrá un sistema específico para la constancia registral de las circunstancias determinantes de la incapacidad para el ejercicio de la Abogacía, la Procura, o la profesión de Graduado Social, así como del plazo durante el que sean de aplicación.

Los Colegios de la Abogacía, Procura y Graduados Sociales están obligados comunicar estas circunstancias a la Administración de Justicia por medios electrónicos, en los términos que se determinen por normativa técnica.

El sistema será además interoperable con los Registros administrativos de apoyo a la Administración de Justicia.

Téngase en cuenta que este apartado 3, modificado por la disposición final 29.1 de la Ley Orgánica 1/2025, de 2 de enero, Ref. BOE-A-2025-76, entra en vigor el 3 de abril de 2025 según establece su disposición final 38.1.

Redacción anterior:

"3. El Registro de Datos de contacto electrónico con la Administración de Justicia dispondrá un sistema específico para la constancia registral de las circunstancias determinantes de la incapacidad para el ejercicio de la Abogacía, la Procura, o la profesión de Graduado Social, así como del plazo durante el que sean de aplicación, con indicación precisa de día inicial y día final.

Los Colegios de la Abogacía, Procura y Graduados Sociales están obligados comunicar estas circunstancias a la Administración de Justicia por medios electrónicos, en los términos que se determinen por normativa técnica.

El sistema será además interoperable con los Registros administrativos de apoyo a la Administración de Justicia."

4. Las personas no obligadas a relacionarse con la Administración de Justicia por medios electrónicos podrán proporcionar sus datos de carácter personal para que se incluyan en el Registro previsto en el presente artículo, pudiendo solicitar la eliminación de los mismos en cualquier momento.

5. El Registro de Datos de contacto electrónico con la Administración de Justicia será interoperable con el sistema de contactos de la Administración General del Estado en los términos que reglamentariamente se establezca.

CAPÍTULO II

Del registro de escritos

Artículo 70. *Registro judicial electrónico.*

1. Las oficinas judiciales con funciones de registro y reparto dispondrán de los medios electrónicos adecuados para la recepción y registro de escritos y documentos, traslado de copias, realización de actos de comunicación y expedición de resguardos electrónicos a través de medios de transmisión seguros, entre los que se incluirán los sistemas de firma y sellado de tiempo basados en certificados electrónicos cualificados.

2. En estos registros judiciales electrónicos únicamente se admitirán escritos y documentos dirigidos a los órganos judiciales, oficinas judiciales y oficinas fiscales adscritos al registro judicial electrónico de que se trate.

3. La recepción de solicitudes, escritos y comunicaciones podrá interrumpirse por el tiempo imprescindible sólo cuando concurran razones justificadas de mantenimiento técnico u operativo. La interrupción deberá anunciarse a los potenciales usuarios y usuarias del registro electrónico con la antelación que, en cada caso, resulte posible. En supuestos de interrupción no planificada en el funcionamiento del registro electrónico, y siempre que sea posible, se dispondrán las medidas para que el usuario o usuaria resulte informado de esta

circunstancia, así como de los efectos de la suspensión, con indicación expresa, en su caso, de la prórroga de los plazos de inminente vencimiento. Alternativamente, podrá establecerse un redireccionamiento que permita utilizar un registro electrónico en sustitución de aquél en el que se haya producido la interrupción.

Artículo 71. *Funcionamiento.*

1. Los registros electrónicos emitirán automáticamente un recibo consistente en una copia autenticada del escrito, documento o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.

2. Los documentos que se acompañen al correspondiente escrito o comunicación deberán cumplir los estándares de formato y requisitos de seguridad que se determinen en el marco institucional de cooperación en materia de administración electrónica. Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados, así como la fecha y hora de presentación y el número de registro de entrada en la correspondiente sede judicial electrónica.

Artículo 72. *Cómputo de plazos.*

1. Los registros electrónicos se regirán, a efectos de cómputo de los plazos imputables tanto a los presentadores como a las oficinas judiciales, por la fecha y hora oficial de la sede judicial electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar visibles. El inicio del cómputo de los plazos que hayan de cumplir los órganos judiciales, oficinas judiciales y oficinas fiscales vendrá determinado por la fecha y hora de presentación en el propio registro.

Téngase en cuenta que este apartado 1, modificado por la disposición final 29.2 de la Ley Orgánica 1/2025, de 2 de enero, Ref. BOE-A-2025-76, entra en vigor el 3 de abril de 2025 según establece su disposición final 38.1.

Redacción anterior:

"1. Los registros electrónicos se regirán, a efectos de cómputo de los plazos imputables tanto a las personas interesadas como a las oficinas judiciales, por la fecha y hora oficial de la sede judicial electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar visibles. El inicio del cómputo de los plazos que hayan de cumplir los órganos judiciales, oficinas judiciales y oficinas fiscales vendrá determinado por la fecha y hora de presentación en el propio registro."

2. Los registros electrónicos permitirán la presentación de escritos, documentos y comunicaciones todos los días del año durante las veinticuatro horas.

3. A los efectos que prevean las leyes procesales en cuanto al cómputo de plazos fijados en días hábiles o naturales, y en lo que se refiere a cumplimiento de plazos por los interesados, la presentación por medios electrónicos, en un día inhábil a efectos procesales conforme a la ley, se entenderá realizada en la primera hora hábil del primer día hábil siguiente, salvo que una norma permita expresamente la recepción en día inhábil.

4. Cada sede judicial electrónica en la que esté disponible un registro electrónico indicará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquélla, los días que se considerarán inhábiles a los efectos de los apartados anteriores.

CAPÍTULO III

Del Registro Electrónico Común de la Administración de Justicia

Artículo 73. *Registro Electrónico Común de la Administración de Justicia.*

1. El Registro Electrónico Común de la Administración de Justicia posibilitará la presentación de escritos y comunicaciones dirigidas a la Administración de Justicia y a los órganos y oficinas judiciales, fiscalías y oficinas fiscales, de manera complementaria e interoperable con los registros existentes en las administraciones con competencia de Justicia.

2. El Registro Electrónico Común de la Administración de Justicia será accesible a través del Punto de Acceso General de la Administración de Justicia e interoperable con el Registro Electrónico Común de la Administración General del Estado.

3. Será gestionado por el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes. El Comité técnico estatal de la Administración judicial electrónica establecerá las condiciones de funcionamiento, así como los requisitos técnicos y previsiones para la adhesión al mismo de los sistemas existentes en las Comunidades Autónomas con competencia en la materia, teniendo el registro electrónico común un carácter complementario a éstos. Los escritos y comunicaciones que reúnan los requisitos que se determinen en la normativa técnica o de desarrollo, presentados al Registro Electrónico Común de la Administración de Justicia, generarán la entrada automática, proporcionando un acuse de recibo electrónico con acreditación de la fecha y hora de presentación.

4. Las administraciones públicas con competencias en medios materiales y personales de la Administración de Justicia facilitarán la interoperabilidad de los sistemas de justicia con el Registro Electrónico Común de la Administración de Justicia.

5. El Registro Electrónico Común de la Administración de Justicia informará al ciudadano, ciudadana o el o la profesional y le redirigirá, cuando proceda, a los registros competentes para la recepción de aquellos documentos que dispongan de aplicaciones o registros específicos para su tratamiento, bien por razón de la materia, bien porque aún no se ha procedido la adhesión de ámbitos competenciales o jurisdiccionales al mismo.

CAPÍTULO IV

Del Registro Electrónico de Apoderamientos Judiciales

Artículo 74. *El Registro Electrónico de Apoderamientos Judiciales.*

1. En el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes existirá un Registro Electrónico de Apoderamientos Judiciales en el que deberán inscribirse los apoderamientos otorgados presencial o electrónicamente por quien ostente la condición de interesado o interesada en un procedimiento judicial a favor de su representante, para actuar en su nombre ante la Administración de Justicia. También deberán constar las demás circunstancias y representaciones previstas en este real decreto-ley.

2. El Registro Electrónico de Apoderamientos Judiciales permitirá comprobar válidamente la representación que ostentan quienes actúen ante la Administración de Justicia en nombre de un tercero.

3. Los asientos que se realicen en el Registro Electrónico de Apoderamientos Judiciales deberán contener, al menos, la siguiente información:

a) Nombre y apellidos o razón social, número de documento nacional de identidad, pasaporte, número de identificación de extranjería o documento de identidad de extranjero si se tratase de una persona extranjera, de identificación fiscal o de documento equivalente del poderdante, domicilio, teléfono y en su caso dirección de correo electrónico.

b) Nombre y apellidos o razón social, número de documento nacional de identidad, pasaporte, NIE, o documento de identidad si se tratase de una persona extranjera, de identificación fiscal o de documento equivalente del apoderado, domicilio, teléfono y en su caso dirección de correo electrónico. En el caso de ser un profesional interviniente ante la Administración de Justicia sometido a colegiación deberá consignarse el número de colegiado y el Colegio Profesional de pertenencia.

c) Fecha de inscripción.
d) Tipo de poder según las facultades que otorgue.

4. Los apoderamientos que se inscriban en el Registro Electrónico de Apoderamientos Judiciales deberán corresponder a alguna de las siguientes tipologías, según el ámbito de los mismos y las facultades conferidas al apoderado o apoderada:

a) Un poder genérico para que el apoderado o apoderada pueda actuar en nombre del poderdante en cualquier clase de procedimiento y actuación judicial.
b) Un poder para que el apoderado o apoderada pueda actuar en nombre del poderdante únicamente en determinadas clases de procedimientos.
c) Un poder específico para que el apoderado o apoderada pueda actuar en nombre del poderdante en un procedimiento concreto.

Las facultades del apoderado podrán ser de carácter general o especial según determine el poderdante, de conformidad con lo establecido en el artículo 25 de Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
5. El poder en que la parte otorgue su representación por comparecencia electrónica, a través de una sede judicial electrónica, en el registro electrónico de apoderamientos judiciales, se efectuará haciendo uso de los sistemas de firma electrónica previstos en este real decreto-ley.
Cuando el poderdante no disponga de sistema de firma electrónica previsto en este real decreto-ley, podrá conferir el poder por comparecencia personal ante el letrado o letrada de la Administración de Justicia de cualquier oficina judicial, debiendo este, en todo caso, asegurar la inscripción en el Registro Electrónico de Apoderamientos Judiciales.
6. Las inscripciones de los apoderamientos en el Registro tendrán una validez determinada máxima de cinco años a contar desde la fecha de inscripción. En todo caso, en cualquier momento antes de la finalización de dicho plazo el poderdante podrá revocar o prorrogar la inscripción. Las prórrogas otorgadas por el poderdante al apoderamiento tendrán una validez determinada máxima de cinco años a contar desde la fecha de inscripción o, en su caso, de la última prórroga.
7. Las solicitudes de revocación, de prórroga o de denuncia del poder podrán dirigirse a cualquier Registro, debiendo quedar inscrita esta circunstancia en el Registro ante el que tenga efectos el poder y surtiendo efectos desde la fecha en la que se produzca dicha inscripción.
8. El tratamiento de los datos deberá ser conforme con la normativa aplicable de protección de datos de carácter personal, incorporándose las medidas técnicas y organizativas necesarias a tal fin.

Artículo 75. *Reconocimiento de las representaciones en el Registro Electrónico de Apoderamientos de la Administración General del Estado.*

1. Los apoderamientos inscritos en el Registro Electrónico de Apoderamientos de la Administración General del Estado previsto en el artículo 6 de la Ley 39/2015, de 1 de octubre, podrán surtir efecto ante los órganos judiciales, oficinas judiciales y oficinas fiscales, en los casos, con los requisitos y con los límites que se determinen por el Comité técnico estatal de la Administración judicial electrónica.
2. En todo caso, será requisito para ello la compatibilidad e interoperabilidad de los sistemas informáticos de los Registros Electrónicos de Apoderamientos Judiciales y de Apoderamientos de la Administración General del Estado, y que el personal al servicio de la Administración de Justicia pueda acceder y consultar el Registro Electrónico de Apoderamientos de la Administración General del Estado.

Artículo 76. *Inscripción del apoderamiento por los representantes procesales.*

Los representantes procesales podrán inscribir directamente el apoderamiento a su favor conferido en aquellos procedimientos que determine el Comité técnico estatal de la Administración judicial electrónica, valorando su cuantía o trascendencia. En el caso de que no pudiere acreditarse el otorgamiento en forma del apoderamiento así inscrito, el que se

hubiera atribuido representación incurrirá en la responsabilidad civil, penal y disciplinaria que derivase de su actuación.

Artículo 77. *Acreditación de la representación procesal.*

La representación procesal se acreditará mediante consulta automatizada orientada al dato que confirme la inscripción de esta en el Registro Electrónico de Apoderamientos Judiciales, cuando el sistema así lo permita. En otro caso, se acreditará mediante la certificación de la inscripción en el Registro Electrónico de Apoderamientos Judiciales.

En todos los casos, quien asuma la representación procesal indicará el número asignado a la inscripción en dicho Registro.

CAPÍTULO V

Registro de personal al servicio de la Administración de Justicia habilitado

Artículo 78. *Registro de personal al servicio de la Administración de Justicia habilitado.*

Podrán ser habilitados los funcionarios y funcionarias al servicio de la Administración de Justicia para la realización por medios electrónicos de trámites, actuaciones o servicios determinados.

Tales habilitaciones se inscribirán en un Registro interoperable con los sistemas de la Administración de Justicia en los términos que se definan por normativa técnica del Comité técnico estatal de la Administración judicial electrónica.

CAPÍTULO VI

Archivos en la Administración de Justicia

Artículo 79. *Sistema de archivo de la Administración de Justicia.*

Las Administraciones públicas con competencias en materias de Administración de Justicia dispondrán de un sistema de archivo judicial electrónico que asegurará el acceso y la conservación a largo plazo de los expedientes y documentos judiciales electrónicos. Este sistema de archivo deberá ser interoperable con todos los sistemas de gestión procesal y demás sistemas de Justicia la prestación del servicio público de Justicia, asegurando unas características y una calidad equivalente en todo el territorio, en los términos que se definan reglamentariamente o mediante normativa técnica del Comité técnico estatal de la Administración judicial electrónica, con respeto a los establecido por la normativa sobre protección de datos de carácter personal. Cada administración con competencias en materia de medios de Justicia deberá determinar si este sistema se provee a través de servicios comunes, a través de las respectivas Sedes electrónicas de cada territorio, o a través de ambos.

Artículo 80. *Documentos en formato no electrónico.*

1. Transcurrido el plazo que se determine reglamentariamente, los documentos en soporte no electrónico que se encuentren en los tribunales, oficinas judiciales y oficinas fiscales y de los que se haya obtenido una copia electrónica auténtica para su registro e incorporación al correspondiente expediente judicial electrónico, podrán ser devueltos a la parte o interesado que los aportó o, en su caso, destruidos, de conformidad con los requisitos que se establezcan en este real decreto-ley o en su desarrollo en vía reglamentaria o normativa técnica.

2. La devolución o, en su caso, la destrucción de los documentos referidos en el apartado anterior se realizará bajo responsabilidad del letrado o letrada de la Administración de Justicia, o por resolución judicial cuando la naturaleza probatoria u otros fines jurisdiccionales así lo aconsejen, previa audiencia de las partes o interesados en todo caso.

TÍTULO VI

Datos abiertos

Artículo 81. *Del Portal de datos de la Administración de Justicia.*

1. El Portal de datos de la Administración de Justicia facilitará a los ciudadanos, ciudadanas y profesionales información procesada y precisa sobre la actividad y carga de trabajo, así como cualesquiera otros datos relevantes, de todos los órganos judiciales, oficinas judiciales y oficinas fiscales, proveída por los sistemas de Justicia en los términos que defina el Comité técnico estatal de la Administración judicial electrónica, con objeto de reflejar la realidad de la Administración de Justicia con el mayor rigor y detalle posibles.

2. La Comisión Nacional de Estadística Judicial determinará la información de estadística judicial que, a los efectos previstos en el apartado anterior, haya de publicarse en el Portal.

3. Dentro de este Portal se incluirá un apartado donde la información tendrá la consideración de «dato abierto».

4. Será necesaria una anonimización previa de los datos garantizando, en todo caso, el nivel de agregación suficiente que impida la identificación de personas físicas.

Artículo 82. *Sobre las condiciones y licencias de reutilización de datos.*

1. Los datos, solicitudes y licencias de reutilización de los datos, que en cumplimiento de lo establecido en el artículo anterior fuesen publicados en el apartado de datos abiertos, estarán sujetos a lo dispuesto en el Real Decreto-ley 24/2021, de 2 de noviembre, de transposición de directivas de la Unión Europea en las materias de bonos garantizados, distribución transfronteriza de organismos de inversión colectiva, datos abiertos y reutilización de la información del sector público, ejercicio de derechos de autor y derechos afines aplicables a determinadas transmisiones en línea y a las retransmisiones de programas de radio y televisión, exenciones temporales a determinadas importaciones y suministros, de personas consumidoras y para la promoción de vehículos de transporte por carretera limpios y energéticamente eficientes.

2. Las administraciones con competencias en materia de Justicia promoverán la utilización, reutilización y compartición de los datos y la información suministrada en los portales con el propósito de favorecer el derecho a la información de los ciudadanos y ciudadanas y el deber de transparencia de los poderes públicos.

3. El tratamiento ulterior de la información no jurisdiccional de datos abiertos o de reutilización de la información a la que se haya accedido en el ámbito jurisdiccional, deberá cumplir la normativa de protección de datos vigente.

Artículo 83. *Datos automáticamente procesables.*

Las Administraciones públicas con competencias en materias de Administración de Justicia velarán por que los datos publicados en el Portal de datos de la Administración de Justicia sean automáticamente procesables siempre que esto sea posible. A tal efecto, los sistemas informáticos de gestión procesal de la Administración de Justicia y sus aplicaciones asociadas habrán de permitir la extracción automatizada de los datos necesarios para la elaboración de la información pública de los portales. Será, en todo caso, responsabilidad de cada Administración con competencias en materia de Justicia el cumplimiento del deber de proporcionar los datos en condiciones idóneas para su empleo en la información de los portales web.

Artículo 84. *Sobre la interoperabilidad de los datos abiertos.*

La parte de datos abiertos del Portal de datos de la Administración de Justicia deberá interoperar con el Portal de datos abiertos del Estado, así como con el de la Unión Europea. Las distintas administraciones pueden usar el Portal de datos de la Administración de Justicia directamente o interoperando los posibles portales propios que tengan al efecto.

TÍTULO VII

Cooperación entre las administraciones con competencias en materia de Administración de Justicia. El Esquema Judicial de Interoperabilidad y Seguridad

CAPÍTULO I

Marco institucional de cooperación en materia de administración electrónica

Artículo 85. *El Comité técnico estatal de la Administración judicial electrónica. Definición y funciones.*

1. El Comité técnico estatal de la Administración judicial electrónica es el órgano de cooperación en materia de Administración judicial electrónica. Estará compuesto por representantes del Consejo General del Poder Judicial, del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, de la Fiscalía General del Estado y de las Comunidades Autónomas con competencias en materias de Administración de Justicia. Está copresidido por un representante del Consejo General del Poder Judicial y otro del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes y tendrá los siguientes fines:

a) El impulso de la cogobernanza de la administración digital de la Justicia.
b) El impulso y coordinación del desarrollo de la transformación digital de la Administración de Justicia.

2. A los fines anteriores, el Comité tendrá las siguientes funciones:

a) Definir y validar la funcionalidad y seguridad de los programas y aplicaciones que se pretendan utilizar el ámbito de la Administración de Justicia, con carácter previo a su implantación.
b) Impulsar y coordinar la elaboración y ejecución de las iniciativas de actuación y planes conjuntos, acuerdos y convenios, en aras a lograr la transformación digital de la Administración de Justicia.
c) Promover la puesta en marcha de servicios interadministrativos integrados y la compartición de infraestructuras técnicas y de los servicios comunes, que permitan la racionalización de los recursos de tecnologías de la información y la comunicación a todos los niveles.
d) Fijar y mantener actualizado el Esquema Judicial de Interoperabilidad y Seguridad, de modo que permita, a través de las plataformas tecnológicas necesarias, la interoperabilidad total de todas las aplicaciones informáticas al servicio de la Administración de Justicia.
e) En materia de ciberseguridad judicial, velar por la seguridad de los sistemas, estableciendo el marco organizativo a través del Subcomité de seguridad, la política de seguridad y promoviendo su desarrollo normativo, así como la definición y establecimiento de criterios de valoración de referencia que permitan a las Administraciones prestacionales determinar el nivel de seguridad de cada dimensión de los sistemas de información de juzgados, tribunales y fiscalías y los niveles de riesgos propuestos por las administraciones instrumentales, en los términos que se establezcan en la normativa relativa a protección de datos y de seguridad aplicable.
f) Informar los anteproyectos de ley, los proyectos de disposiciones reglamentarias y otras normas, que le sean sometidas por los órganos proponentes y cuyo objeto sea la regulación en materia de tecnologías de la información y la comunicación de aplicación en la Administración de Justicia.
g) Aquellas otras que legal o reglamentariamente se determinen.

Artículo 86. *Relaciones con otros órganos.*

1. El Comité técnico estatal de la Administración judicial electrónica y la Conferencia Sectorial de Justicia se coordinarán en el ejercicio de sus funciones, en aras de la eficiencia de los servicios públicos. A tal fin se arbitrarán los mecanismos de colaboración que correspondan.

2. Dentro del modelo de gobernanza, con el objetivo de aunar esfuerzos y coordinar la ejecución del proceso de transformación digital, se fijará un marco de colaboración constante entre la Administración General del Estado y sus organismos y entidades de Derecho Público vinculadas o dependientes, y el Comité técnico estatal de la Administración judicial electrónica.

Dicha colaboración se articulará a través del Comité de Dirección para la Digitalización de la Administración u órgano equivalente.

3. Asimismo, con objeto de cumplir con el mandato contenido en el artículo 461 de la Ley Orgánica 6/1985, de 1 de julio, se arbitrarán los mecanismos de coordinación necesarios entre la Comisión Nacional de Estadística Judicial y el Comité técnico estatal de la Administración judicial electrónica.

Artículo 87. *Consejo Consultivo para la Transformación Digital de la Administración de Justicia.*

1. Las administraciones públicas con competencias en Justicia favorecerán que la iniciativa, diseño, desarrollo y producción de sistemas se lleven a cabo en colaboración con el sector privado y los colectivos principalmente afectados.

2. A tal fin, se constituirá un Consejo Consultivo del que formen parte:

a) Organizaciones sindicales.

b) Asociaciones profesionales de jueces y juezas, fiscales y letrados y letradas de la Administración de Justicia.

c) Consejos Generales de la Abogacía, la Procura y los Graduados y Graduadas Sociales.

d) Asociaciones y Organizaciones Empresariales, así como la asociación o asociaciones de empresas de electrónica, tecnologías de la información, telecomunicaciones y digitalización.

e) El Colegio Oficial de Registradores de la Propiedad y Mercantiles de España.

f) El Consejo General del Notariado.

g) La Federación Española de Municipios y Provincias.

h) Secretaría General de Administración Digital.

i) Las demás organizaciones que se determinen a los fines de este artículo.

En el caso de las Administraciones con competencias transferidas en materia de justicia se podrán crear Consejos territoriales, cuya composición se adecuará a los representantes institucionales, colegiales y asociativos de cada territorio.

CAPÍTULO II

Esquema Judicial de Interoperabilidad y Seguridad

Sección 1.ª Interoperabilidad judicial

Artículo 88. *Esquema Judicial de Interoperabilidad y Seguridad.*

1. El Esquema Judicial de Interoperabilidad y Seguridad estará constituido por el conjunto de instrucciones técnicas de interoperabilidad y seguridad aprobadas por el Comité técnico estatal de la Administración judicial electrónica y que permitan el cumplimiento del Esquema Nacional de Interoperabilidad y del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, recogiendo las particularidades de la Administración de Justicia que requieran una concreta regulación.

2. Los indicados esquemas nacionales y sus instrucciones técnicas de desarrollo serán de obligado cumplimiento, sin perjuicio de las adaptaciones indicadas en el apartado anterior.

3. Asimismo, forma parte del Esquema Judicial de Interoperabilidad y Seguridad el conjunto de instrucciones técnicas que dicte el Comité técnico estatal de la Administración judicial electrónica en el ejercicio de sus competencias de conformidad con la Ley Orgánica 6/1985, de 1 de julio, y el presente real decreto-ley.

4. Las instrucciones técnicas indicadas en los apartados anteriores se denominarán guías técnicas de interoperabilidad y seguridad.

5. El Esquema Judicial de Interoperabilidad y Seguridad, previo análisis de los riesgos incorporará las medidas técnicas y organizativas destinadas a garantizar y poder acreditar que el tratamiento de los datos de carácter personal es conforme con la normativa de protección de datos personales que serán revisadas y actualizadas cuando sea necesario.

Artículo 89. *Interoperabilidad de los sistemas de información.*

Los sistemas de información y comunicación que se utilicen en la Administración de Justicia deberán ser interoperables entre sí para facilitar su comunicación e integración, en los términos que determine el Comité técnico estatal de la Administración judicial electrónica.

A fin de asegurar la interoperabilidad a la que se refiere el apartado anterior, corresponderá al Comité técnico estatal de la Administración judicial electrónica identificar y definir los metadatos mínimos obligatorios que deben contener los documentos judiciales y los metadatos complementarios. Los sistemas de Justicia asegurarán en todo caso la incorporación, entrada y tratamiento, como mínimo, de los metadatos mínimos obligatorios, tanto en los intercambios entre sistemas de la Administración correspondiente, como en los intercambios con otras administraciones públicas con competencias en medios materiales y personales de la Administración de Justicia, y con otras administraciones públicas.

En el ámbito del presente real decreto-ley, será de obligado cumplimiento el Esquema Nacional de Interoperabilidad, así como la normativa europea de interoperabilidad aplicable. Para adecuar su cumplimiento, y en caso de requerir una regulación específica de acuerdo con las particularidades propias de la Administración de Justicia, el Comité técnico estatal de la Administración judicial electrónica desarrollará normas técnicas de interoperabilidad que serán de obligado cumplimiento, a través de guías técnicas de interoperabilidad y seguridad de dicho Comité.

Artículo 90. *Consejos Generales y profesiones colegiadas.*

Las aplicaciones y servicios electrónicos que los Consejos Generales de la Abogacía, de la Procura y de Graduados y Graduadas Sociales pongan a disposición de los y las profesionales deberán interoperar con los sistemas de gestión procesal, si fuera necesario a través de los servicios comunes a todas las administraciones competentes previstos en este real decreto-ley.

Reglamentariamente, previo informe del Comité técnico estatal de la Administración judicial electrónica, oídos los Consejos Generales, se establecerán para todo el ámbito estatal las condiciones y funcionalidades obligatorias de la interoperabilidad.

Artículo 91. *Notarías y Registros de la Propiedad, Bienes Muebles y Mercantiles y cualesquiera otros Registros Públicos con los que se relaciona la Administración de Justicia y el resto de administraciones públicas y sus organismos públicos y entidades de derecho público vinculadas y dependientes.*

Los registros electrónicos a disposición de los Registros de la Propiedad, Mercantiles y de Bienes Muebles, y cualesquiera otros Registros Públicos con los que se relaciona la Administración de Justicia, así como el protocolo electrónico de las Notarías, garantizarán la accesibilidad y consulta, para fines jurisdiccionales, desde los órganos judiciales, oficinas judiciales y oficinas fiscales, y la interoperabilidad con los sistemas de gestión procesal, si fuera necesario a través de los servicios comunes a todas las administraciones competentes previstos en este real decreto-ley, posibilitando la automatización de interacciones habituales entre el órgano judicial y el Registro o el órgano judicial y la Notaría, que no exijan el ejercicio de la función calificadora ni de la fe pública.

La interconexión se hará por un protocolo electrónico de accesibilidad y consulta, que será único para toda la Administración de Justicia, bajo acuerdo del Comité técnico estatal de la Administración judicial electrónica.

Del mismo modo, los registros electrónicos a los que se refiere este precepto, garantizarán la interoperabilidad con los sistemas utilizados por el resto de administraciones

públicas, y sus organismos públicos y entidades de derecho público vinculadas y dependientes conforme a la normativa que sea de aplicación en cada caso.

Artículo 92. *Cooperación jurídica internacional y comunicaciones electrónicas transfronterizas.*

1. Las comunicaciones entre los órganos judiciales unipersonales y colegiados, así como Fiscalía y las oficinas judiciales y fiscales, y el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, relativas a actos de cooperación jurídica internacional se realizarán por medios electrónicos que aseguren el cumplimiento de los requisitos técnicos establecidos en el presente real decreto-ley y los requisitos procesales y de contenido establecidos en el marco normativo vigente. Se exceptúan los casos en los que el Estado de destino no admita las comunicaciones electrónicas.

2. A tal fin, las administraciones públicas con competencias en medios materiales y personales de la Administración de Justicia implantarán soluciones que permitan la comunicación electrónica de datos y documentos entre los juzgados y tribunales, así como las oficinas judiciales y oficinas fiscales, y el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, en los términos previstos en el apartado anterior. Estas soluciones serán interoperables con los sistemas de gestión procesal y posibilitarán la entrada, incorporación y tratamiento de la información en forma de metadatos, conforme a esquemas comunes, y en modelos de datos.

3. Los sistemas informáticos de gestión procesal de la Administración de Justicia permitirán la extracción automatizada de los datos relativos al sistema judicial cuando por el derecho de la Unión Europea o tratado internacional en vigor el Estado esté obligado a comunicarlos a organismos internacionales. El Ministerio de la Presidencia, Justicia y Relaciones con las Cortes centralizará la información a los fines de su remisión al organismo correspondiente.

Sección 2.ª Ciberseguridad judicial

Artículo 93. *Política de seguridad de la información de la Administración Judicial Electrónica.*

1. Corresponde al Comité técnico estatal de la Administración judicial electrónica la elaboración y actualización de la política de seguridad de la información de la Administración de Justicia, en sus aspectos organizativos, técnicos, físicos y de cumplimiento de la normativa.

2. Esta política de seguridad de la información será de aplicación a todos los sistemas de información y comunicaciones que prestan servicios a la Administración de Justicia, de manera única, y será aprobada por el Comité técnico estatal de la Administración judicial electrónica y publicada en el Punto de Acceso General de la Administración de Justicia y en las sedes judiciales electrónicas.

Téngase en cuenta que este apartado 2, modificado por la disposición final 29.3 de la Ley Orgánica 1/2025, de 2 de enero, Ref. BOE-A-2025-76, entra en vigor el 3 de abril de 2025 según establece su disposición final 38.1.

Redacción anterior:

"2. Esta política de seguridad de la información será de aplicación a todos los sistemas de información y comunicaciones que prestan servicios a la Administración de Justicia, de manera única, y será aprobada por el Comité técnico estatal de la Administración judicial electrónica y publicada como acuerdo del órgano de cooperación en el «Boletín Oficial del Estado» y en los Boletines o Diarios Oficiales de las Comunidades Autónomas con competencias asumidas en materia de Justicia, así como en el Punto de Acceso General de la Administración de Justicia y en las sedes judiciales electrónicas."

3. Sin perjuicio de la declaración de conformidad y la certificación con el Esquema Nacional de Seguridad, los sistemas de información de la Administración de Justicia deberán acreditar su conformidad con el Esquema Judicial de Interoperabilidad y Seguridad, de acuerdo con los términos que se establezcan en el Comité técnico estatal de la Administración judicial electrónica.

4. Las entidades del sector privado que provean de soluciones o presten servicios a las administraciones, a sus organismos y a las instituciones sometidas al presente real decreto-ley, deberán estar a lo dispuesto en esta política de seguridad, así como al cumplimiento con los esquemas nacionales de interoperabilidad y seguridad, las guías de interoperabilidad y seguridad, y las instrucciones técnicas de seguridad del Comité técnico estatal de la Administración judicial electrónica que sean aplicables.

Artículo 94. *Mejora continua del proceso de seguridad.*

1. El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica y estándares nacionales e internacionales relativos a gestión de las tecnologías de la información.

2. El Esquema Judicial de Interoperabilidad y Seguridad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de administración electrónica, de la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que lo apoyan. Para ello, se desarrollarán las correspondientes guías y normas técnicas de aplicación.

3. Corresponde al Comité técnico estatal de la Administración judicial electrónica aprobar las bases para la actualización del Esquema Judicial de Interoperabilidad y Seguridad.

Artículo 95. *Subcomité de Seguridad.*

1. El Subcomité de Seguridad es el órgano especializado y permanente para la ciberseguridad judicial del Comité técnico estatal de la Administración judicial electrónica.

2. El Subcomité de Seguridad estará integrado por aquellas personas con responsabilidad en materia de seguridad de cada una de las administraciones e instituciones integrantes del Comité técnico estatal de la Administración judicial electrónica, así como por las personas que designe el Consejo General del Poder Judicial y la Fiscalía General del Estado. Se arbitrarán los mecanismos de colaboración necesarios entre el Subcomité de Seguridad y el Centro Criptológico Nacional.

3. Por vía reglamentaria se establecerán las funciones del Subcomité de Seguridad, que tendrán por objeto principal el establecimiento de un marco común de cooperación que permita la adopción de decisiones comunes y coordinadas en materia de ciberseguridad judicial.

4. El Comité técnico estatal de la Administración judicial electrónica se apoyará en el Subcomité de Seguridad para la elaboración de las instrucciones técnicas y guías de interoperabilidad y seguridad necesarias, en cumplimiento del Esquema Nacional de Seguridad, así como de la normativa en materia de protección de datos de carácter personal.

Artículo 96. *Centro de Operaciones de Ciberseguridad de la Administración de Justicia.*

El Centro de Operaciones de Ciberseguridad de la Administración de Justicia reforzará las capacidades de vigilancia, prevención, protección, detección, respuesta ante incidentes de ciberseguridad, asesoramiento y apoyo a la gestión de la ciberseguridad de un modo centralizado, que permita una mejor eficacia y eficiencia.

Para conseguirlo, el Centro de Operaciones de Ciberseguridad de la Administración de Justicia prestará un conjunto de servicios horizontales de ciberseguridad a las administraciones públicas prestatarias del servicio público de Justicia.

La gestión de estos servicios incluirá, fundamentalmente, la implantación de la infraestructura técnica y herramientas, los procedimientos, la operación y otras cuestiones asociadas. En el caso de las Administraciones con competencias en ciberseguridad y servicios horizontales para los sistemas de la Administración de Justicia, y dentro de la actividad del Comité Técnico Estatal de la Administración Judicial Electrónica, se crearán

grupos de trabajo en los que se concretarán los datos a intercambiar y los medios de colaboración que se consideren necesarios.

El Centro de Operaciones de Ciberseguridad de la Administración de Justicia articulará la respuesta a los incidentes de seguridad, y actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada Administración con competencias en materia de Justicia e instituciones judiciales sometidas al presente real decreto-ley, y de la función de coordinación a nivel nacional e internacional del Equipo de Respuesta para Emergencias Informáticas del Centro Criptológico Nacional (CCN-CERT).

CAPÍTULO III

Reutilización de aplicaciones y transferencia de tecnologías. Directorio general de información tecnológica judicial

Artículo 97. *Reutilización de sistemas, infraestructuras y aplicaciones de propiedad de las administraciones con competencias en materia de Justicia.*

1. Las administraciones titulares de los derechos de propiedad intelectual de aplicaciones, desarrolladas por sus servicios o cuyo desarrollo haya sido objeto de contratación, las pondrán a disposición de cualquier institución judicial o cualquier Administración Pública sin contraprestación y sin necesidad de convenio.

2. Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración de Justicia. Se publicarán, en tal caso, como licencia pública de la Unión Europea, sin perjuicio de otras licencias que aseguren que los programas, datos o información que se comparten:

a) Pueden ejecutarse para cualquier propósito.
b) Permiten conocer su código fuente.
c) Pueden modificarse o mejorarse.
d) Pueden redistribuirse a otros usuarios con o sin cambios, siempre que la obra derivada mantenga estas mismas cuatro garantías.

3. Las administraciones públicas con competencias en Justicia, con carácter previo a la adquisición, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, deberán consultar en el directorio general de aplicaciones del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, y en su caso, deberán consultar en el directorio general de aplicaciones, dependiente de la Administración General del Estado, si existen soluciones disponibles para su reutilización, que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

En el caso de existir una solución disponible para su reutilización total o parcial, las administraciones públicas con competencias en medios materiales y personales de la Administración de Justicia podrán reutilizarla previa formalización de convenio de acuerdo con lo establecido en el artículo 47 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Artículo 98. *Transferencia de tecnología entre administraciones. Directorio general de información tecnológica judicial.*

1. El Ministerio de la Presidencia, Justicia y Relaciones con las Cortes mantendrá un directorio general de aplicaciones judiciales para su reutilización e impulsará el mantenimiento del mismo, en colaboración con el resto de administraciones públicas con competencias en materia de Justicia. Se promoverá el desarrollo de guías técnicas, formatos y estándares comunes de especial interés para el desarrollo de la Administración judicial electrónica en el marco institucional de cooperación en materia de administración electrónica.

2. Las distintas administraciones mantendrán directorios actualizados de aplicaciones para su libre reutilización, especialmente en aquellos campos de especial interés para el

desarrollo de la administración electrónica y de conformidad con lo que al respecto se establezca en el marco institucional de cooperación en materia de administración electrónica.

3. Las administraciones con competencias en materia de Justicia deberán tener en cuenta las soluciones disponibles para la libre reutilización que puedan satisfacer total o parcialmente las necesidades de los nuevos sistemas y servicios o la mejora y actualización de los ya implantados. En concreto, podrán adherirse voluntariamente y a través de medios electrónicos a las plataformas, aplicaciones y registros establecidos.

CAPÍTULO IV

Protección de datos de carácter personal

Artículo 99. *Protección de datos en el uso de los medios tecnológicos e informáticos.*

Los sistemas que se utilicen en la Administración de Justicia y que traten datos personales que vayan a ser incorporados a un proceso judicial o expediente fiscal para fines jurisdiccionales se ajustarán a la normativa prevista en los artículos 236 bis a 236 decies de la Ley Orgánica 6/1985, de 1 de julio; en el artículo 2, párrafos 4 y 5, de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 2.2 de la Ley Orgánica 7/2021, de 26 de mayo.

Artículo 100. *Protección de datos en los documentos judiciales electrónicos.*

Las oficinas judiciales y fiscales dispondrán de los medios tecnológicos adecuados para la realización automatizada de la anonimización, seudonimización y disociación de los datos de carácter personal.

Con la finalidad de posibilitar lo dispuesto en el párrafo anterior, las resoluciones procesales y judiciales deberán adecuarse a un formato normalizado acordado en el seno del Comité técnico estatal de la Administración judicial electrónica.

[. . .]

Disposición adicional primera. *Interoperabilidad entre las aplicaciones de la Administración de Justicia.*

En el plazo de cinco años desde la entrada en vigor del libro primero del presente real decreto-ley, las administraciones públicas con competencias en medios materiales y personales de la Administración de Justicia garantizarán la interoperabilidad entre los sistemas al servicio de la Administración de Justicia, de acuerdo con lo previsto en el presente real decreto-ley, en sus desarrollos reglamentarios y en las especificaciones establecidas por el Comité Técnico Estatal de Administración Judicial Electrónica en el marco institucional de cooperación en materia de administración electrónica.

Disposición adicional segunda. *Accesibilidad a los servicios electrónicos en el ámbito de la Administración de Justicia.*

Las administraciones con competencias en materia de Justicia garantizarán que todos los ciudadanos y ciudadanas, con especial atención a las personas mayores o personas con algún tipo de discapacidad, que se relacionan con la Administración de Justicia, puedan acceder a los servicios electrónicos en igualdad de condiciones con independencia de sus circunstancias personales, medios o conocimientos.

A tal fin, se ajustarán en lo que sea de aplicación al Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público y demás regulación estatal y autonómica en materia de igualdad y no discriminación.

Disposición adicional tercera. *Dotación de medios e instrumentos electrónicos a la Administración de Justicia.*

Las administraciones públicas competentes en materia de Justicia dotarán a todos los órganos judiciales, oficinas judiciales y oficinas fiscales de los medios e instrumentos electrónicos necesarios y suficientes para poder desarrollar su función eficientemente. Asimismo, formarán a sus integrantes en el uso y utilización de dichos medios e instrumentos.

Disposición adicional cuarta. *Aplicación en el ámbito de la jurisdicción militar del libro primero del real decreto-ley.*

Las disposiciones contenidas en el libro primero del presente real decreto-ley serán de aplicación en el ámbito de la jurisdicción militar sin perjuicio de las especialidades propias de sus normas reguladoras.

Disposición adicional quinta. *Declaración de requerimientos tecnológicos de las reformas en las leyes procesales.*

Todo anteproyecto de ley de reformas de leyes procesales deberá ir acompañado, cuando proceda, de una declaración de requerimientos tecnológicos para su correcta implantación y aplicación.

Disposición adicional sexta. *Instrumentos de desarrollo normativo aprobados por el Comité técnico estatal de la Administración judicial electrónica.*

Las guías de interoperabilidad y seguridad de las tecnologías de la información y las comunicaciones que sean aprobadas en el seno del Comité técnico estatal de la Administración judicial electrónica serán obligatorias para cada una de las instituciones y administraciones con competencias en materia de Justicia a través de sus instrumentos normativos, de conformidad con sus competencias.

Téngase en cuenta que esta modificación, establecida por la disposición final 29.4 de la Ley Orgánica 1/2025, de 2 de enero, Ref. BOE-A-2025-76, entra en vigor el 3 de abril de 2025 según determina su disposición final 38.1.

Redacción anterior:

"**Disposición adicional sexta. Instrumentos de desarrollo normativo aprobados por el Comité técnico estatal de la Administración judicial electrónica.**

Las guías de interoperabilidad y seguridad de las tecnologías de la información y las comunicaciones que sean aprobadas en el seno del Comité técnico estatal de la Administración judicial electrónica serán obligatorias para cada una de las instituciones y administraciones con competencias en materia de Justicia a través de sus instrumentos normativos, de conformidad con sus competencias, y serán publicadas en sus Boletines o Diarios Oficiales correspondientes para su plena eficacia jurídica."

Disposición adicional séptima. *Sistemas de identificación y firma no criptográficos admitidos con anterioridad en el ámbito de la Administración de Justicia.*

1. Seguirán siendo válidos aquellos sistemas de identificación y sistemas de firma no criptográficos que hayan sido admitidos por el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes y por las Comunidades Autónomas con competencias transferidas, y establecidos de acuerdo con la legislación básica estatal, la Ley 39/2015, de 1 de octubre, o conforme a la misma. Asimismo, seguirán siendo válidos aquellos sistemas establecidos de conformidad con el artículo 14.2 c) de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, siempre que hayan sido regulados y publicados en los respectivos boletines o diarios oficiales.

2. Será de aplicación lo establecido en la disposición adicional sexta de la Ley 39/2015, de 1 de octubre.

Disposición adicional octava. *Soluciones tecnológicas para garantizar la efectividad de los servicios y sistemas previstos en el libro primero del presente real decreto-ley.*

El Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, las demás administraciones públicas con competencias transferidas de medios materiales y personales de la Administración de Justicia, el Consejo General del Poder Judicial, la fiscalía General del Estado, los Consejos de los Colegios profesionales, y cualesquiera otras administraciones o Instituciones adoptarán todas las medidas necesarias a fin de garantizar la puesta en marcha, para que sean efectivos los servicios y sistemas previstos en el libro primero del presente real decreto-ley.

Disposición adicional novena. *Personal de los Cuerpos Generales y Especiales de la Administración de Justicia.*

En atención a la imprescindible implicación de los profesionales de los Cuerpos Generales y Especiales de la Administración de Justicia en el proceso de transformación comprometido en el Plan Estratégico «Justicia 2030» y en el Plan de Recuperación, Transformación y Resiliencia, y con el objetivo de lograr una mejora de la eficiencia organizativa, procesal y digital en aras de una administración más ágil, eficiente, adaptada a la ciudanía, sostenible y transparente, y puesto que este proceso de transformación tiene una especial incidencia en la adaptación de las funciones que realizan estos profesionales, por el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes se llevarán a cabo las actuaciones precisas para reconocer e identificar esta incidencia.

[. . .]

Disposición transitoria primera. *Coexistencia de procedimientos judiciales tramitados en soporte papel y en formato electrónico.*

1. Durante el tiempo en que coexistan procedimientos tramitados en soporte papel con procedimientos tramitados exclusivamente en formato electrónico, los servicios electrónicos de información del estado de la tramitación a que se refiere el libro primero del presente real decreto-ley incluirán respecto a los primeros, al menos, la fase en la que se encuentra el procedimiento y el órgano o unidad responsable de su tramitación.

2. Los registros electrónicos existentes a la entrada en vigor del libro primero del presente real decreto-ley serán considerados registros judiciales electrónicos y se regularán por lo dispuesto en ella.

Disposición transitoria segunda. *Régimen transitorio aplicable a los procedimientos judiciales.*

Las previsiones recogidas por el libro primero del presente real decreto-ley serán aplicables exclusivamente a los procedimientos judiciales incoados con posterioridad a su entrada en vigor, salvo que en este se disponga otra cosa.

Disposición transitoria tercera. *Expediente electrónico con valor de copia simple.*

Si el estado de la técnica no hiciera posible remitir el expediente administrativo electrónico con los requisitos establecidos en este real decreto-ley y en la normativa técnica de aplicación, y, en todo caso, hasta el plazo máximo de los cinco años siguientes a la entrada en vigor del libro primero del presente real decreto-ley, será admisible la remisión del expediente en otro formato digital que posibilite su descarga y reutilización por el tribunal, oficina judicial u oficina fiscal. El expediente así remitido tendrá valor de copia simple.

[. . .]

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, así como todas las normas de igual o inferior rango en lo que contradigan o se opongan a lo dispuesto en el presente real decreto-ley.

[. . .]

Disposición final novena. *Entrada en vigor.*

1. El presente real decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

2. El libro primero, las disposiciones adicionales primera a novena, y las disposiciones transitorias primera a tercera entrarán en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

No obstante, las previsiones contenidas en el título VIII del libro primero y en las disposiciones finales primera, segunda y cuarta, entrarán en vigor a los tres meses de su publicación en el «Boletín Oficial del Estado».

3. El libro cuarto entrará en vigor el 1 de enero del año 2024.

4. Desde la entrada en vigor del libro primero del presente real decreto-ley, los servicios y sistemas tecnológicos previstos en el mismo o que sean necesarios para la plena operatividad de sus preceptos, serán plenamente aplicables en todas las Comunidades Autónomas que ya cuenten con los mismos.

5. Las Comunidades Autónomas que aún no cuenten con tales sistemas o servicios, o que, contando con los mismos, aún no hayan operado su plena integración con los nodos, servicios o sistemas comunes del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes deberán, en todo caso, llevar a cabo su plena aplicación e integración el 30 de noviembre de 2025.

A tal fin, desarrollarán todas las actuaciones necesarias para disponer de los mismos y su plena integración, en los plazos convenidos en el marco de la Conferencia Sectorial de Justicia para la distribución y reparto del crédito asignado en el Mecanismo de Recuperación y Resiliencia.

En concreto, deberán realizar estas actuaciones de conformidad con los acuerdos publicados por Resolución de 14 de junio de 2022, de la Secretaría de Estado de Justicia, por la que se publica el Acuerdo de la Conferencia Sectorial de Administración de Justicia, por el que se formalizan los criterios de distribución y el reparto resultante para las Comunidades Autónomas, del crédito asignado en el año 2022 y en el año 2023 por el Mecanismo de Recuperación y Resiliencia, y se formalizan los compromisos financieros resultantes, y por Resolución de 27 de marzo de 2023, de la Secretaría de Estado de Justicia, por la que se publica el Acuerdo de la Conferencia Sectorial de Administración de Justicia, por el que se modifica el reparto resultante para las Comunidades Autónomas del crédito asignado para el año 2023 del Mecanismo de Recuperación y Resiliencia y se formalizan los compromisos financieros resultantes.

[. . .]

ANEXO

Definiciones

A efectos del presente real decreto-ley, se entiende por:

Aplicación: programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de la informática.

Aplicación de fuentes abiertas: aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios.

Autenticación: acreditación por medios electrónicos de la identidad de una persona o ente, del contenido de la voluntad expresada en sus operaciones, transacciones y documentos y de la integridad y autoría de estos últimos.

Autenticación del interviniente: acto realizado por el Tribunal, oficina judicial u oficina fiscal que tiene por objetivo reforzar la identificación de las actuaciones que se lleven a cabo por medios electrónicos.

Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Canales: estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro.

Certificado de firma electrónica: según el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.

Certificado cualificado de firma electrónica: según el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I de dicha norma. Ciberseguridad (seguridad de los sistemas de información): De conformidad con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, es la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Datos abiertos: de conformidad con el anexo de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, son aquellos que cualquiera es libre de utilizar, reutilizar y redistribuir, con el único límite, en su caso, del requisito de atribución de su fuente o reconocimiento de su autoría.

Disponibilidad: propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Dispositivo electrónico: aparato formado por la combinación de diferentes elementos electrónicos con capacidad de procesamiento y conexión a una red que permite el envío y recepción de información entre usuarios.

Dirección electrónica: identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones.

Documento electrónico: información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Estándar abierto: aquel que reúna las siguientes condiciones: que sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso y cuyos uso y aplicación no estén condicionados al pago de un derecho de propiedad intelectual o industrial.

Firma electrónica: según el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

Firma electrónica avanzada: según el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, la firma electrónica que cumple los requisitos contemplados en el artículo 26.

Firma electrónica reconocida: según el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

Índice electrónico: relación de documentos electrónicos de un expediente electrónico, firmada por la Administración, órgano o entidad actuante, según proceda y cuya finalidad es garantizar la integridad del expediente electrónico y permitir su recuperación siempre que sea preciso.

Infraestructuras y servicios comunes: Instrumentos operativos que facilitan el desarrollo y despliegue de nuevos servicios, así como la interoperabilidad de los existentes, creando escenarios de relación multilateral y que satisfacen las necesidades comunes en los distintos ámbitos administrativos; son ejemplos la Red de comunicaciones de las administraciones públicas españolas, la Red transeuropeas-TESTA y la plataforma de verificación de certificados electrónicos.

Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Interoperabilidad: capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Licencia pública de la Unión Europea («European Union Public Licence-EUPL»): licencia adoptada oficialmente por la Comisión Europea en las veintitrés lenguas oficiales comunitarias para reforzar la interoperabilidad de carácter legal mediante un marco colectivo para la puesta en común de las aplicaciones del sector público.

Medidas de seguridad: conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción o de recuperación.

Medio electrónico: mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

Metadato: dato que define y describe otros datos, existiendo diferentes tipos de metadatos según su aplicación.

Metadato de gestión de documentos: información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

Profesionales que se relacionen con la Administración de Justicia: operadores jurídicos que, teniendo funciones de defensa, representación, peritaje, interpretación o cualesquiera otras que se determinen en las leyes procesales, sin pertenecer a ella por vínculos funcionariales o laborales, se relacionen de forma habitual con la Administración de Justicia.

Punto de acceso electrónico: conjunto de páginas web agrupadas en un dominio de Internet cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios dirigidos a resolver necesidades específicas de un grupo de personas o el acceso a la información y servicios de una institución pública.

Requisitos mínimos de seguridad: exigencias necesarias para asegurar la información y los servicios.

Sistema de firma electrónica: conjunto de elementos intervinientes en la creación de una firma electrónica. En el caso de la firma electrónica basada en certificado electrónico, componen el sistema, al menos, el certificado electrónico, el soporte, el lector, la aplicación de firma utilizada y el sistema de interpretación y verificación utilizado por el receptor del documento firmado.

Sello electrónico: según el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

Sello electrónico avanzado: según el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, un sello electrónico que cumple los requisitos contemplados en el artículo 36 de dicho Reglamento.

Sello electrónico reconocido: según el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.

Sellado de tiempo: acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Sello de tiempo: la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Sistema de información: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Sistemas de Código Seguro de Verificación: procedimientos basados en un código que identifica a un documento electrónico y cuya finalidad es garantizar el origen e integridad de los documentos mediante el acceso a la sede electrónica correspondiente; el carácter único del código generado para cada documento; su vinculación con el documento generado, de forma que cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente; la posibilidad de verificar el documento en la sede electrónica como mínimo por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento; así como un acceso al documento restringido a quien disponga del código seguro de verificación.

Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Información relacionada

- El Real Decreto-ley 6/2023, de 19 de diciembre, ha sido convalidado por Acuerdo del Congreso de los Diputados, publicado por Resolución de 10 de enero de 2024. Ref. BOE-A-2024-665