2024/2982

4.12.2024

REGLAMENTO DE EJECUCIÓN (UE) 2024/2982 DE LA COMISIÓN

de 28 de noviembre de 2024

por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los protocolos y las interfaces que admitirá el marco europeo de identidad digital

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto 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 ([1]), y, en particular, su artículo 5 *bis*, apartado 23,

Considerando lo siguiente:

(1) El marco europeo de identidad digital establecido por el Reglamento (UE) n.º 910/2014 es un componente crucial para la creación de un ecosistema de identidad digital seguro e interoperable en toda la Unión. El objetivo de este marco, con las carteras europeas de identidad digital (en lo sucesivo, las «carteras») como piedra angular, es facilitar el acceso a los servicios en todos los Estados miembros, para las personas físicas y jurídicas, garantizando al mismo tiempo la protección de los datos personales y de la privacidad.

(2) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([2]) y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([3]) son aplicables a todas las actividades de tratamiento de datos personales en virtud del presente Reglamento.

(3) El artículo 5 *bis*, apartado 23, del Reglamento (UE) n.º 910/2014 encomienda a la Comisión que, en caso necesario, establezca las especificaciones y los procedimientos pertinentes. Este mandato se lleva a cabo mediante cuatro Reglamentos de Ejecución, que tratan respectivamente de los protocolos y las interfaces: Reglamento de Ejecución (UE) 2024/2982 de la Comisión ([4]), la integridad y las funcionalidades básicas: Reglamento de Ejecución (UE) 2024/2979 de la Comisión ([5]), los datos de identificación de la persona y la declaración electrónica de atributos: Reglamento de Ejecución (UE) 2024/2977 de la Comisión ([6]), y las notificaciones a la Comisión: Reglamento de Ejecución (UE) 2024/2980 de la Comisión ([7]). El presente Reglamento establece los requisitos pertinentes para los protocolos y las interfaces.

([1]) DO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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), DO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

([3]) 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, ELI: http://data.europa.eu/eli/dir/2002/58/oj.

([4]) Reglamento de Ejecución 2024/2982 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los protocolos y las interfaces que admitirá el marco europeo de identidad digital (DO L, 2024/2982, 4.12.2024 ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Reglamento de Ejecución (UE) 2024/2979 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la integridad y las funcionalidades básicas de las carteras europeas de identidad digital (DO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Reglamento de Ejecución (UE) 2024/2977 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los datos de identificación de la persona y las declaraciones electrónicas de atributos expedidos a carteras europeas de identidad digital, DO L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Reglamento de Ejecución (UE) 2024/2980, de 28 de noviembre de 2024, de la Comisión, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las notificaciones a la Comisión relativas al ecosistema de la cartera europea de identidad digital, DO L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) La Comisión evalúa periódicamente las nuevas tecnologías, prácticas, normas y especificaciones técnicas. Con el fin de garantizar el máximo nivel de armonización entre los Estados miembros para el desarrollo y la certificación de las carteras, las especificaciones técnicas establecidas en el presente Reglamento se basan en el trabajo realizado con arreglo a la Recomendación (UE) 2021/946 de la Comisión, de 3 de junio de 2021, sobre un conjunto de instrumentos común de la Unión para adoptar un enfoque coordinado de cara a un Marco para una Identidad Digital Europea ([8]), y en particular la arquitectura y el marco de referencia. De conformidad con el considerando 75 del Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo ([9]), la Comisión debe revisar y, en caso necesario, actualizar el presente Reglamento de Ejecución, para mantenerlo en consonancia con la evolución mundial, la arquitectura y el marco de referencia, y seguir las mejores prácticas en el mercado interior.

(5) A fin de garantizar la transparencia y la fiabilidad de las partes usuarias de una cartera ante los usuarios de una cartera, los protocolos y las interfaces utilizados por las soluciones de cartera deben proporcionar a sus usuarios un mecanismo fiable para autenticar a las partes usuarias de una cartera y otras unidades de cartera. Por su parte, los proveedores de carteras deben proporcionar un mecanismo para autenticar y validar las unidades de cartera que ofrezca a las partes usuarias garantías respecto a la fiabilidad y la autenticidad de las unidades de cartera. Además, la infraestructura técnica de las carteras debe estar diseñada también para garantizar que solo se transfiera la cantidad mínima necesaria de datos y únicamente a las partes usuarias autorizadas, manteniendo la no vinculación entre las diferentes transacciones. Con el fin de facilitar la expedición de datos de identificación de la persona y declaraciones electrónicas de atributos, todas las soluciones de cartera deben admitir un conjunto mínimo de protocolos e interfaces.

(6) Para garantizar la facilidad de uso de las soluciones de cartera en todos los Estados miembros, todas las soluciones de cartera deben atenerse a unas especificaciones técnicas comunes cuando los datos de identificación de la persona y las declaraciones electrónicas de atributos se presenten a través de las carteras a las partes usuarias, tanto a distancia como en escenarios de proximidad. Además, las unidades de cartera pueden admitir otros protocolos e interfaces para casos de uso específicos.

(7) Para garantizar la protección de datos mediante el diseño y por defecto, las carteras deben estar provistas de varias características de mejora de la privacidad que impidan que los proveedores de medios de identificación electrónica y declaraciones electrónicas de atributos combinen los datos personales que obtengan cuando presten otros servicios con los datos personales tratados para prestar los servicios incluidos en el ámbito de aplicación del Reglamento (UE) n.º 910/2014. Tal como se establece en el Reglamento (UE) n.º 910/2014, las partes usuarias no deben solicitar a los usuarios que faciliten otros datos que no sean los indicados para el uso previsto de las carteras durante el proceso de registro. Conviene que los usuarios de una cartera puedan verificar en cualquier momento los datos de registro de las partes usuarias. Además, conviene que las unidades de cartera puedan mostrar a los usuarios los certificados de registro de las partes usuarias de la cartera, cuando se disponga de ellos, como parte de una solicitud de atributos. Esto debe permitir a los usuarios de una cartera verificar que los atributos que les solicita la parte usuaria de la cartera están dentro del ámbito de sus atributos registrados, lo que ofrece garantías de que la solicitud es legítima y fiable.

(8) Con el fin de proteger los datos de los usuarios de una cartera, los proveedores de carteras deben garantizar que las unidades de cartera validen las solicitudes de las partes usuarias de la cartera u otras unidades de cartera antes de facilitar dato alguno. Por la misma razón, y de conformidad con el artículo 5 *bis*, apartado 4, letra d), inciso ii), del Reglamento (UE) n.º 910/2014, los proveedores de carteras deben garantizar que las unidades de cartera permitan a los usuarios de una cartera solicitar la supresión de datos a las partes usuarias de la cartera.

(9) A fin de permitir una reacción rápida en caso de problemas de protección de datos relacionados con el artículo 5 *bis*, apartado 4, letra d), inciso iii), del Reglamento (UE) n.º 910/2014, los proveedores de carteras deben garantizar que las soluciones de cartera proporcionen mecanismos para denunciar a una parte usuaria ante la autoridad nacional competente de protección de datos. Debe concederse a los proveedores de carteras y las autoridades de protección de datos la flexibilidad adecuada a la hora de establecer los mecanismos adecuados para interactuar con las autoridades de protección de datos de los Estados miembros.

(10) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([10]), emitió su dictamen el 30 de septiembre de 2024.

([8]) DO L 210 de 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (DO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([10]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(11) Las medidas previstas en el presente Reglamento se ajustan al dictamen del comité contemplado en el artículo 48, del Reglamento (UE) n.º 910/2014,

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Objeto y ámbito de aplicación

El presente Reglamento establece normas sobre los protocolos y las interfaces de las soluciones de cartera para:

1) la expedición de datos de identificación de la persona y declaraciones electrónicas de atributos a unidades de cartera;

2) la presentación de atributos de los datos de identificación de la persona y las declaraciones electrónicas de atributos a las partes usuarias de la cartera y a otras unidades de cartera;

3) la comunicación de las solicitudes de supresión de datos a las partes usuarias de la cartera;

4) la denuncia de partes usuarias de la cartera ante las autoridades de control establecidas en virtud del artículo 51 del Reglamento (UE) 2016/679;

que deben actualizarse periódicamente para mantenerlos en consonancia con la evolución de la tecnología y las normas y con el trabajo realizado sobre la base de la Recomendación (UE) 2021/946, y en particular la arquitectura y el marco de referencia.

Artículo 2

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «parte usuaria de la cartera»: parte que tiene la intención de utilizar unidades de cartera para la prestación de servicios públicos o privados mediante interacción digital;

2) «usuario de una cartera»: usuario que tiene el control sobre la unidad de cartera;

3) «solución de cartera»: combinación de *software*, *hardware*, servicios, ajustes y configuraciones, que incluye instancias de cartera, una o más aplicaciones criptográficas seguras de cartera y uno o más dispositivos criptográficos seguros de cartera;

4) «unidad de cartera»: configuración única de una solución de cartera que incluye instancias de cartera, aplicaciones criptográficas seguras de cartera y dispositivos criptográficos seguros de cartera proporcionados por un proveedor de carteras a un usuario particular de una cartera;

5) «proveedor de cartera»: persona física o jurídica que proporciona soluciones de cartera;

6) «instancia de cartera»: aplicación instalada y configurada en el dispositivo o el entorno de un usuario de una cartera, que forma parte de una unidad de cartera y que el usuario de la cartera utiliza para interactuar con la unidad de cartera;

7) «aplicación criptográfica segura de cartera»: aplicación que gestiona activos críticos al estar vinculada a las funciones criptográficas y no criptográficas proporcionadas por el dispositivo criptográfico seguro de cartera y utilizarlas;

8) «dispositivo criptográfico seguro de cartera»: dispositivo resistente a las manipulaciones fraudulentas que proporciona un entorno vinculado a la aplicación criptográfica segura de cartera y utilizado por esta para proteger activos críticos y proporcionar funciones criptográficas para la ejecución segura de operaciones críticas;

9) «activos críticos»: activos contenidos en una unidad de cartera o relacionados con ella, de tan extraordinaria importancia que si su disponibilidad, confidencialidad o integridad se vieran comprometidas, el efecto sobre la capacidad para utilizar la unidad de cartera sería muy grave y debilitante;

10) «certificado de acceso de partes usuarias de la cartera»: certificado para sellos o firmas electrónicos, expedido por un proveedor de certificados de acceso de partes usuarias de la cartera, que autentica y valida a la parte usuaria de cartera;

11) «proveedor de certificados de acceso de partes usuarias de la cartera»: persona física o jurídica a la que un Estado miembro ha encomendado expedir certificados de acceso de parte usuaria a las partes usuarias de la cartera registradas en ese Estado miembro;

12) «declaración de unidad de cartera»: objeto de datos que describe los componentes de la unidad de cartera o permite la autenticación y la validación de esos componentes;

13) «política de divulgación incorporada»: conjunto de normas, incorporadas en una declaración electrónica de atributos por su proveedor, que indica las condiciones que debe cumplir una parte usuaria de la cartera para acceder a la declaración electrónica de atributos;

14) «certificado de registro de partes usuarias de la cartera»: objeto de datos que indica los atributos que la parte usuaria ha registrado con el propósito de solicitárselos a los usuarios;

15) «proveedor de datos de identificación de la persona»: persona física o jurídica responsable de la expedición y la revocación de los datos de identificación de la persona y de garantizar que los datos de identificación de la persona de un usuario estén vinculados criptográficamente a una unidad de cartera;

16) «vinculación criptográfica»: método para vincular los datos de identificación de la persona o las declaraciones electrónicas de atributos a unidades de cartera por medios criptográficos.

Artículo 3

Disposiciones generales

Por lo que respecta a los protocolos y las interfaces a que se refieren los artículos 4 y 5, los proveedores de carteras se asegurarán de que las unidades de cartera:

1) autentiquen y validen los certificados de acceso de la parte usuaria de la cartera cuando interactúen con partes usuarias de la cartera;

2) autentiquen y validen las declaraciones de unidad de cartera de otras unidades de cartera cuando interactúen con otras unidades de cartera;

3) autentiquen y validen las solicitudes realizadas utilizando certificados de acceso de parte usuaria de la cartera o declaraciones de unidad de cartera de otras unidades de cartera, cuando proceda;

4) autentiquen y validen el certificado de registro de la parte usuaria de la cartera, cuando proceda;

5) muestren a los usuarios de una cartera la información contenida en los certificados de acceso de la parte usuaria de la cartera o en las declaraciones de unidad de cartera;

6) muestren a los usuarios de una cartera, cuando proceda, los atributos que se les exige que presenten;

7) muestren a los usuarios de una cartera, cuando proceda, la información contenida en el certificado de registro de la parte usuaria de la cartera;

8) presenten las declaraciones de unidad de cartera de la unidad de cartera a las partes usuarias de la cartera o las unidades de cartera que lo soliciten;

9) no presenten ningún atributo solicitado a las partes usuarias de la cartera ni a las unidades de cartera hasta que se cumplan los siguientes requisitos:

   a) verificar que la aplicación criptográfica segura de cartera ha autenticado la identidad del usuario de una cartera;

   b) verificar que las políticas de divulgación incorporadas han sido procesadas en la unidad de cartera de conformidad con el artículo 11 del Reglamento de Ejecución (UE) 2024/2979, cuando proceda;

   c) verificar que los usuarios de una cartera han aprobado total o parcialmente la presentación;

10) permitan técnicas de protección de la privacidad que garanticen la no vinculación en los casos en que las declaraciones electrónicas de atributos no exijan la identificación del usuario de una cartera, cuando presenten declaraciones o datos de identificación de la persona a diferentes partes usuarias de la cartera.

Artículo 4

Expedición de datos de identificación de la persona y declaraciones electrónicas de atributos a unidades de cartera

1. Los proveedores de carteras se asegurarán de que las soluciones de cartera admitan protocolos e interfaces para la expedición de datos de identificación de la persona y declaraciones electrónicas de atributos a unidades de cartera.

2. Los proveedores de carteras se asegurarán de que las unidades de cartera soliciten la expedición de datos de identificación de la persona y declaraciones electrónicas de atributos únicamente a partes que tengan un certificado de acceso de parte usuaria de la cartera auténtico y válido que las acredite como:

a) proveedor de datos de identificación de la persona;

b) proveedor de una declaración electrónica cualificada de atributos;

c) proveedor de una declaración electrónica de atributos expedida por un organismo del sector público responsable de una fuente auténtica, o en nombre de este; o

d) proveedor de declaraciones electrónicas no cualificadas de atributos.

3. En relación con la expedición de datos de identificación de la persona y declaraciones electrónicas de atributos a una unidad de cartera, los proveedores de carteras se asegurarán de que se cumplan los siguientes requisitos:

a) cuando los usuarios de una cartera utilicen su unidad de cartera para solicitar la expedición de datos de identificación de la persona o de declaraciones electrónicas de atributos a los proveedores de datos de identificación de la persona o de declaraciones electrónicas de atributos que permitan la expedición de dichos datos o dichas declaraciones en más de un formato, la unidad de la cartera la solicitará en todos los formatos a que se refiere el artículo 8 del Reglamento de Ejecución (UE) 2024/2979, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 en lo que respecta a la integridad y las funcionalidades básicas de las carteras europeas de identidad digital;

b) cuando los usuarios de una cartera utilicen su unidad de cartera para interactuar con proveedores de datos de identificación de la persona o declaraciones electrónicas de atributos, las unidades de cartera permitirán la autenticación y validación de los componentes de la unidad de cartera mediante la presentación de las declaraciones de unidad de cartera a dichos proveedores cuando lo soliciten;

c) las soluciones de cartera admitirán mecanismos que permitan a los proveedores de datos de identificación de la persona verificar la expedición, la entrega y la activación de conformidad con los requisitos del nivel de seguridad alto establecidos en el Reglamento de Ejecución (UE) 2015/1502 de la Comisión ([11]);

d) las unidades de la cartera verificarán la autenticidad y la validez de los datos de identificación de la persona y de las declaraciones electrónicas de atributos.

Artículo 5

Presentación de atributos a las partes usuarias de la cartera

1. Los proveedores de carteras se asegurarán de que las soluciones de cartera admitan protocolos e interfaces para la presentación de atributos a las partes usuarias de la cartera, a distancia y, cuando proceda, en proximidad, de conformidad con las normas establecidas en el anexo.

2. Los proveedores de carteras se asegurarán de que, a petición de los usuarios, las unidades de cartera respondan a las solicitudes autenticadas y validadas de las partes usuarias de la cartera a que se refiere el artículo 3, de conformidad con las normas establecidas en el anexo.

3. Los proveedores de carteras se asegurarán de que las unidades de cartera admitan la demostración de la posesión de claves privadas correspondientes a claves públicas utilizadas en las vinculaciones criptográficas.

([11]) Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DO L 235 de 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

4. Los proveedores de carteras se asegurarán de que las soluciones de cartera admitan la divulgación selectiva de atributos de datos de identificación de la persona y de declaraciones electrónicas de atributos.

5. Los apartados 1 a 4 se aplicarán *mutatis mutandis* a las interacciones entre dos unidades de cartera que se encuentren próximas.

Artículo 6

Comunicación de solicitudes de supresión de datos

1. Los proveedores de carteras se asegurarán de que las unidades de cartera admitan protocolos e interfaces que permitan a los usuarios de una cartera solicitar a las partes usuarias de la cartera con las que hayan interactuado a través de dichas unidades de cartera la supresión de sus datos personales facilitados a través de dichas unidades de cartera, de conformidad con el artículo 17 del Reglamento (UE) 2016/679.

2. Los protocolos y las interfaces a que se refiere el apartado 1 permitirán a los usuarios de una cartera seleccionar las partes usuarias de la cartera a las que deben presentarse las solicitudes de supresión de datos.

3. Las unidades de cartera mostrarán al usuario de una cartera las solicitudes de supresión de datos presentadas previamente a través de dichas unidades.

Artículo 7

Denuncia de partes usuarias de la cartera ante las autoridades de control establecidas en virtud del artículo 51 del Reglamento (UE) 2016/679

1. Los proveedores de carteras se asegurarán de que las unidades de cartera permitan a los usuarios de una cartera denunciar fácilmente a las partes usuarias de la cartera ante las autoridades de control establecidas en virtud del artículo 51 del Reglamento (UE) 2016/679.

2. Los proveedores de carteras aplicarán los protocolos y las interfaces pertinentes para denunciar a las partes usuarias de la cartera de conformidad con el Derecho procesal nacional de los Estados miembros.

3. Los proveedores de carteras se asegurarán de que las unidades de cartera permitan a sus usuarios fundamentar sus denuncias, en particular adjuntando información pertinente para identificar a las partes usuarias de la cartera, y hacer sus reclamaciones en un formato legible por máquina.

Artículo 8

Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 28 de noviembre de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

NORMAS A LAS QUE SE HACE REFERENCIA EN EL ARTÍCULO 5, APARTADOS 1 Y 2

— ISO/IEC 18013-5:2021

— ISO/IEC TS 18013-7:2024