DECISIÓN DE EJECUCIÓN (UE) 2022/483 DE LA COMISIÓN

de 21 de marzo de 2022

que modifica la Decisión de Ejecución (UE) 2021/1073 por la que se establecen especificaciones técnicas y normas relativas a la aplicación del marco de confianza para el certificado COVID digital de la UE establecido por el Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo, de 14 de junio de 2021, relativo a un marco para la expedición, verificación y aceptación de certificados COVID-19 interoperables de vacunación, de prueba diagnóstica y de recuperación (certificado COVID digital de la UE) a fin de facilitar la libre circulación durante la pandemia de COVID-19 ([1]), y en particular su artículo 9, apartado 1,

Considerando lo siguiente:

(1) El Reglamento (UE) 2021/953 establece el certificado COVID digital de la UE, que acredita que una persona ha recibido una vacuna contra la COVID-19, un resultado negativo de una prueba diagnóstica o se ha recuperado de la infección, con el fin de facilitar el ejercicio, por parte de los titulares, de su derecho a la libre circulación durante la pandemia de COVID-19.

(2) El Reglamento (UE) 2021/954 del Parlamento Europeo y del Consejo ([2]) establece que los Estados miembros deben aplicar las normas establecidas en el Reglamento (UE) 2021/953 a los nacionales de terceros países que no entren en el ámbito de aplicación de dicho Reglamento pero se encuentren o residan legalmente en su territorio y tengan derecho a viajar a otros Estados miembros de conformidad con el Derecho de la Unión.

(3) La Recomendación (UE) 2022/290 del Consejo ([3]) establece que los nacionales de terceros países que deseen realizar viajes no esenciales desde un tercer país a la Unión deben estar en posesión de una prueba válida de vacunación o recuperación, como un certificado COVID digital de la UE o un certificado COVID-19 expedido por un tercer país cubierto por un acto de ejecución adoptado con arreglo al artículo 8, apartado 2, del Reglamento (UE) 2021/953.

(4) Para que el certificado COVID digital de la UE funcione en toda la Unión, la Comisión adoptó la Decisión de Ejecución (UE) 2021/1073 ([4]) por la que se establecen especificaciones técnicas y normas que permitan cumplimentar, expedir y verificar de forma segura los certificados COVID digitales, garantizar la protección de los datos personales, establecer una estructura común del identificador único del certificado y expedir un código de barras válido, seguro e interoperable.

(5) De conformidad con el artículo 4 del Reglamento (UE) 2021/953, la Comisión y los Estados miembros debían establecer y mantener un marco de confianza para el certificado COVID digital de la UE. El marco de confianza puede apoyar el intercambio bilateral de listas de revocación de certificados que contengan los identificadores únicos de los certificados revocados.

([1]) DO L 211 de 15.6.2021, p. 1.

([2]) Reglamento (UE) 2021/954 del Parlamento Europeo y del Consejo, de 14 de junio de 2021, relativo a un marco para la expedición, verificación y aceptación de certificados COVID-19 interoperables de vacunación, de prueba diagnóstica y de recuperación (certificado COVID digital de la UE) con respecto a los nacionales de terceros países que se encuentren o residan legalmente en los territorios de los Estados miembros durante la pandemia de COVID-19 (DO L 211 de 15.6.2021, p. 24).

([3]) Recomendación (UE) 2022/290 del Consejo, de 22 de febrero de 2022, por la que se modifica la Recomendación (UE) 2020/912 sobre la restricción temporal de los viajes no esenciales a la UE y el posible levantamiento de dicha restricción (DO L 43 de 24.2.2022, p. 79).

([4]) Decisión de Ejecución (UE) 2021/1073 de la Comisión, de 28 de junio de 2021, por la que se establecen especificaciones técnicas y normas relativas a la aplicación del marco de confianza para el certificado COVID digital de la UE establecido por el Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo (DO L 230 de 30.6.2021, p. 32).

(6) El 1 de julio de 2021 entró en funcionamiento la pasarela del certificado COVID digital de la UE (en lo sucesivo, «pasarela»), que es la parte central del marco de confianza y que permite el intercambio seguro y fiable entre los Estados miembros de las claves públicas utilizadas para verificar los certificados COVID digitales de la UE.

(7) Debido al éxito y la gran escala de su implantación, los certificados COVID digitales de la UE se han convertido en un objetivo para los defraudadores que intentan encontrar formas de expedir certificados fraudulentos. Por lo tanto, esos certificados fraudulentos deben ser revocados. Además, algunos certificados COVID digitales de la UE pueden ser revocados por los Estados miembros a nivel nacional por motivos médicos y de salud pública, por ejemplo, porque se haya constatado posteriormente que un lote de vacunas administradas era defectuoso.

(8) Si bien el sistema de certificados COVID digitales de la UE tiene la capacidad de revelar inmediatamente aquellos que son falsificados, los certificados auténticos expedidos ilegalmente sobre la base de documentación falsa, acceso no autorizado o intención fraudulenta no pueden detectarse en otros Estados miembros a menos que los Estados miembros intercambien las listas de certificados revocados generados a nivel nacional. Lo mismo se aplica a los certificados que han sido revocados por razones médicas y de salud pública. El hecho de que las solicitudes de verificación de los Estados miembros no detecten los certificados revocados por otros Estados miembros supone una amenaza para la salud pública y socava la confianza de los ciudadanos en el sistema de certificados COVID digitales de la UE.

(9) Como se señala en el considerando 19 del Reglamento (UE) 2021/953, los Estados miembros deben, por motivos médicos y de salud pública y en el caso de certificados expedidos u obtenidos de forma fraudulenta, poder establecer e intercambiar con otros Estados miembros, a los efectos de dicho Reglamento, listas de revocación de certificados en casos limitados, en particular en lo que respecta a los certificados que se hayan expedido de forma incorrecta, fraudulenta o tras la suspensión de un lote defectuoso de vacunas contra la COVID-19. Los Estados miembros no deben tener la posibilidad de revocar los certificados expedidos por otros Estados miembros. Las listas de revocación de certificados intercambiadas no deberán contener ningún dato personal distinto del identificador único de certificado. En particular, no deben incluir el motivo por el que se ha revocado un certificado.

(10) Además de la información general sobre la posibilidad de revocación de certificados y los posibles motivos para ello, los titulares de certificados revocados deben ser informados sin demora por la autoridad expedidora responsable acerca de la revocación de sus certificados y de los motivos de la misma. Sin embargo, en determinados casos, y en particular en el caso de los certificados COVID digitales de la UE expedidos en papel, localizar al titular e informarle de la revocación puede resultar imposible o implicar un esfuerzo desproporcionado. Los Estados miembros no deben recopilar datos personales adicionales que no sean necesarios para el proceso de expedición únicamente con el objetivo de poder informar a los titulares de certificados en caso de revocación de estos.

(11) Por tanto, es necesario mejorar el marco de confianza del certificado COVID digital de la UE apoyando el intercambio bilateral de listas de revocación de certificados entre los Estados miembros.

(12) La presente Decisión no cubre la suspensión temporal de certificados para casos de uso nacional fuera del ámbito de aplicación del Reglamento sobre el certificado COVID digital de la UE, por ejemplo porque el titular de un certificado de vacunación haya dado positivo en una prueba diagnóstica del SARS-CoV-2. Esto se entiende sin perjuicio de los procedimientos establecidos para la comprobación de las normas comerciales relativas a la validez de los certificados.

(13) Aunque, desde un punto de vista técnico, son viables diferentes arquitecturas para el intercambio de listas de revocación, la forma más adecuada de hacerlo es a través de la pasarela, ya que limita los intercambios de datos al marco de confianza ya establecido y minimiza el número tanto de posibles puntos de fallo como de intercambios entre Estados miembros, en comparación con un sistema alternativo entre pares.

(14) En consecuencia, debe mejorarse la pasarela del certificado COVID digital de la UE para apoyar el intercambio seguro de certificados COVID digitales de la UE revocados a efectos de su verificación segura a través de la pasarela. A este respecto, deben aplicarse medidas de seguridad adecuadas para proteger los datos personales tratados en la pasarela. Para garantizar un elevado nivel de protección, los Estados miembros deben seudonimizar los atributos del certificado mediante un hash irreversible que se incluya en las listas de revocación. De hecho, el identificador único debe considerarse como dato seudonimizado para las operaciones de procesamiento realizadas en el marco de la pasarela.

(15) Además, deben establecerse disposiciones adicionales relativas a la función de los Estados miembros y de la Comisión en lo que respecta al intercambio de listas de revocación de certificados.

(16) El tratamiento de los datos personales de los titulares de certificados, efectuado bajo la responsabilidad de los Estados miembros o de otras organizaciones públicas u organismos oficiales de los Estados miembros, debe llevarse a cabo de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([5]). El tratamiento de datos personales bajo la responsabilidad de la Comisión con el fin de gestionar y garantizar la seguridad de la pasarela del certificado COVID digital de la UE debe cumplir lo dispuesto en el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([6]).

(17) Los Estados miembros, representados por las autoridades nacionales o los organismos oficiales designados, determinan conjuntamente el propósito y los medios de tratamiento de los datos personales a través de la pasarela del certificado COVID digital de la UE, por lo que son corresponsables del tratamiento. El artículo 26 del Reglamento (UE) 2016/679 impone a los corresponsables de las operaciones de tratamiento de datos personales la obligación de determinar de manera transparente sus responsabilidades respectivas en el cumplimiento de las obligaciones establecidas en dicho Reglamento. También contempla la posibilidad de que tales responsabilidades se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. El acuerdo a que se refiere el artículo 26 debe incluirse en el anexo III de la presente Decisión.

(18) El Reglamento (UE) 2021/953 encomienda a la Comisión la tarea de apoyar dichos intercambios. La forma más adecuada de cumplir este mandato es recopilar las listas de revocación de certificados presentadas en nombre de los Estados miembros. Por consiguiente, debe asignarse a la Comisión una función de encargada del tratamiento de datos para apoyar estos intercambios facilitando el intercambio de listas a través de la pasarela del certificado COVID digital de la UE en nombre de los Estados miembros.

(19) La Comisión, en su calidad de proveedora de soluciones técnicas y organizativas para la pasarela del certificado COVID digital de la UE, trata los datos personales de las listas de revocación en la pasarela en nombre de los Estados miembros en tanto que corresponsables del tratamiento. Por lo tanto, actúa como encargada del tratamiento de dichos datos. Según el artículo 28 del Reglamento (UE) 2016/679 y el artículo 29 del Reglamento (UE) 2018/1725, el tratamiento por el 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 respecto del responsable del tratamiento y que especifique el tratamiento. Por consiguiente, resulta necesario establecer normas que rijan el tratamiento efectuado por la Comisión como encargada del tratamiento de datos.

(20) La tarea de apoyo de la Comisión no implica la creación de una base de datos central como la mencionada en el considerando 52 del Reglamento (UE) 2021/953. Esa prohibición tiene por objeto evitar que exista un repositorio central de todos los certificados COVID digitales de la UE expedidos y no impide que los Estados miembros intercambien listas de revocación, lo que el artículo 4, apartado 2, del Reglamento (UE) 2021/953 prevé de forma expresa.

(21) Al tratar datos personales en el marco de la pasarela del certificado COVID digital de la UE, la Comisión debe atenerse a lo dispuesto en su Decisión (UE, Euratom) 2017/46 ([7]).

(22) El artículo 3, apartado 10, del Reglamento (UE) 2021/953 permite a la Comisión adoptar actos de ejecución por los que se establezca que los certificados COVID-19 expedidos por un tercer país con el que la Unión y los Estados miembros hayan celebrado un acuerdo en materia de libre circulación de personas que permita a las partes contratantes restringir la libre circulación por motivos de salud pública de manera no discriminatoria y que no contenga un mecanismo de incorporación de actos jurídicos de la Unión son equivalentes a los expedidos de conformidad con el presente Reglamento. Sobre esa base, la Comisión adoptó, el 8 de julio de 2021, la Decisión de Ejecución (UE) 2021/1126 ([8]), por la que se establece la equivalencia de los certificados COVID-19 expedidos por Suiza.

([5]) 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).

([6]) 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).

([7]) La Comisión Europea publica más información sobre las normas de seguridad aplicables a todos sus sistemas de información en https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_es.

([8]) Decisión de Ejecución (UE) 2021/1126 de la Comisión, de 8 de julio de 2021, por la que se establece la equivalencia entre los certificados COVID-19 expedidos por Suiza y los certificados expedidos de conformidad con el Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo (DO L 243 de 9.7.2021, p. 49).

(23) El artículo 8, apartado 2, del Reglamento (UE) 2021/953 permite a la Comisión adoptar actos de ejecución por los que se establezca que los certificados COVID-19 expedidos por un tercer país con arreglo a normas y sistemas tecnológicos que sean interoperables con el marco de confianza para el certificado COVID digital de la UE, que permitan verificar la autenticidad, validez e integridad del certificado, y que contengan los datos establecidos en el anexo al Reglamento, deben ser considerados equivalentes a los certificados COVID digitales de la UE, a fin de facilitar a sus titulares el ejercicio de su derecho a la libre circulación en la Unión. Como se indica en el considerando 28 del Reglamento (UE) 2021/953, el artículo 8, apartado 2, de dicho Reglamento se refiere a la aceptación de certificados expedidos por terceros países a ciudadanos de la Unión y a los miembros de sus familias. La Comisión ya ha adoptado varios actos de ejecución de este tipo.

(24) Para evitar lagunas en la detección de los certificados revocados que se contemplan en dichos actos de ejecución, también debe ser posible que los terceros países cuyos certificados COVID-19 se hayan considerado equivalentes con arreglo al artículo 3, apartado 10, y al artículo 8, apartado 2, del Reglamento (UE) 2021/953 presenten las listas pertinentes de revocación de certificados en la pasarela del certificado COVID digital de la UE.

(25) Algunos nacionales de terceros países que tienen certificados de COVID-19 revocados emitidos por un tercer país y considerados equivalentes con arreglo al artículo 3, apartado 10, y al artículo 8, apartado 2, del Reglamento (UE) 2021/953, pueden entrar en el ámbito de aplicación de ese Reglamento o del Reglamento (UE) 2021/954 en el momento en que el tercer país en cuestión genera una lista de revocación que incluye sus certificados. No obstante, no puede saberse, en el momento en que un tercer país en cuestión genera una lista de revocación de certificados, si todos los nacionales de terceros países que son titulares de certificados revocados entran en el ámbito de aplicación de cualquiera de esos Reglamentos. El intento de excluir a las personas no incluidas en el ámbito de aplicación de dichos Reglamentos en el momento en que se generan las listas de revocación de certificados de esos países no es, por tanto, viable y, al intentar hacerlo, los Estados miembros no podrían detectar los certificados revocados de los que sean titulares nacionales de terceros países que viajen por primera vez a la Unión. No obstante, incluso los certificados revocados de esos nacionales de terceros países serían verificados por los Estados miembros cuando sus titulares viajen a la Unión y, seguidamente, cuando viajen dentro de la Unión. Los terceros países cuyos certificados se hayan considerado equivalentes con arreglo al Reglamento (UE) 2021/953 no participan en la gobernanza de la pasarela y, por tanto, no pueden considerarse corresponsables del tratamiento.

(26) Además, el sistema de certificado COVID digital de la UE ha demostrado ser el único sistema de certificados COVID-19 operativo a gran escala y de ámbito internacional. Por ello, el certificado COVID digital de la UE ha adquirido una creciente importancia en el mundo y ha contribuido a hacer frente a la pandemia a nivel internacional, facilitando unos viajes internacionales seguros y una recuperación global. En el proceso de adopción de actos de ejecución adicionales de conformidad con el artículo 8, apartado 2, del Reglamento (UE) 2021/953, surgen nuevas necesidades en relación con la cumplimentación del certificado COVID digital de la UE. De conformidad con las normas establecidas en la Decisión de Ejecución (UE) 2021/1073, los apellidos son un campo obligatorio del contenido técnico del certificado. Es necesario modificar ese requisito para favorecer la inclusión y la interoperabilidad con otros sistemas, puesto que en algunos terceros países hay personas sin apellidos. En los casos en que el nombre del titular del certificado no pueda separarse en dos partes, el nombre debe colocarse en el mismo campo (apellidos o nombre) del certificado COVID digital de la UE en que se indicaría en el documento de viaje o de identidad del titular. Con este cambio también se ajustaría mejor el contenido técnico de los certificados a las especificaciones actualmente vigentes sobre documentos de viaje de lectura mecánica publicadas por la Organización de Aviación Civil Internacional.

(27) Procede, por tanto, modificar la Decisión de Ejecución (UE) 2021/1073 en consecuencia.

(28) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725, emitió su dictamen el 11 de marzo de 2022.

(29) A fin de que los Estados miembros y la Comisión dispongan de tiempo suficiente para aplicar los cambios necesarios que permitan el intercambio de listas de revocación de certificados a través de la pasarela del certificado COVID digital de la UE, la presente Decisión debe empezar a aplicarse cuatro semanas después de su entrada en vigor.

(30) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité creado por el artículo 14 del Reglamento (UE) 2021/953.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

La Decisión de Ejecución (UE) 2021/1073 se modifica como sigue:

1) Se insertan los artículos 5 *bis*, 5 *ter* y 5 *quater* siguientes:

«*Artículo 5 bis*

Intercambio de listas de revocación de certificados

1. El marco de confianza para el certificado COVID digital de la UE permitirá el intercambio de listas de revocación de certificados a través de la pasarela central del certificado COVID digital de la UE ("pasarela"), de conformidad con las especificaciones técnicas del anexo I.

2. Cuando los Estados miembros revoquen los certificados COVID digitales de la UE, podrán presentar listas de revocación de certificados en la pasarela.

3. Cuando los Estados miembros presenten listas de revocación de certificados, las autoridades expedidoras mantendrán una lista de certificados revocados.

4. Cuando los datos personales se intercambien a través de la pasarela, la finalidad de su tratamiento se limitará a apoyar el intercambio de información relativa a la revocación. Dichos datos personales solo se utilizarán para verificar el estado de revocación de los certificados COVID digitales de la UE expedidos en el ámbito de aplicación del Reglamento (UE) 2021/953.

5. La información presentada en la pasarela incluirá los siguientes datos, de conformidad con las especificaciones técnicas establecidas en el anexo I:

a) los identificadores únicos de certificado seudonimizados de los certificados revocados;

b) una fecha de expiración de la lista de revocación de certificados que se ha presentado.

6. Cuando una autoridad expedidora revoque certificados COVID digitales de la UE que ella misma haya expedido en virtud del Reglamento (UE) 2021/953 o del Reglamento (UE) 2021/954, y tenga la intención de intercambiar información pertinente a través de la pasarela, transmitirá la información a que se refiere el apartado 5 en forma de listas de revocación de certificados en la pasarela en un formato seguro, de conformidad con las disposiciones técnicas establecidas en el anexo I.

7. Las autoridades expedidoras proporcionarán, en la medida de lo posible, una solución para informar a los titulares de certificados revocados sobre el estado de revocación de sus certificados y el motivo de la revocación en el momento que esta se produzca.

8. La pasarela recopilará las listas de revocación de certificados recibidas. Proporcionará herramientas para la distribución de las listas a los Estados miembros. Suprimirá automáticamente las listas de conformidad con las fechas de caducidad indicadas por la autoridad en cuestión para cada lista que haya presentado.

9. Las autoridades nacionales o los organismos oficiales designados de los Estados miembros que traten datos personales en la pasarela serán corresponsables del tratamiento de dichos datos. Las respectivas responsabilidades de los corresponsables del tratamiento se asignarán de acuerdo con el anexo VI.

10. La Comisión será la encargada del tratamiento de los datos personales tratados dentro de la pasarela. En su calidad de encargada del tratamiento de los datos en nombre de los Estados miembros, la Comisión garantizará la seguridad de la transmisión y del alojamiento de datos personales en la pasarela y cumplirá las obligaciones del encargado del tratamiento establecidas en el anexo VII.

11. La eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento de los datos personales en la pasarela será sometida a ensayo, valorada y evaluada con regularidad por la Comisión y por los corresponsables del tratamiento.

Artículo 5 ter

Presentación de listas de revocación de certificados por terceros países

Los terceros países que expidan certificados COVID-19 respecto de los cuales la Comisión haya adoptado un acto de ejecución con arreglo al artículo 3, apartado 10, o al artículo 8, apartado 2, del Reglamento (UE) 2021/953 podrán presentar en la pasarela listas de certificados COVID-19 revocados cubiertos por dicho acto de ejecución para que sean tratadas por la Comisión en nombre de los corresponsables del tratamiento, tal como se refiere en el artículo 5 *bis*, de conformidad con las especificaciones técnicas establecidas en el anexo I.

Artículo 5 quater

Gobernanza del tratamiento de datos personales en la pasarela central del certificado COVID digital de la UE

1. El proceso de toma de decisiones de los corresponsables del tratamiento se regirá por un grupo de trabajo creado en el marco del Comité a que se refiere el artículo 14 del Reglamento (UE) 2021/953.

2. Las autoridades nacionales o los organismos oficiales designados de los Estados miembros que traten datos personales en la pasarela como corresponsables de su tratamiento designarán representantes en dicho grupo.».

2) El anexo I se modifica de conformidad con el anexo I de la presente Decisión.

3) El anexo V se modifica de conformidad con el anexo II de la presente Decisión.

4) El texto que figura en el anexo III de la presente Decisión se añade como anexo VI.

5) El texto que figura en el anexo IV de la presente Decisión se añade como anexo VII.

Artículo 2

La presente Decisión entrará en vigor a los tres días de su publicación en el *Diario Oficial de la Unión Europea*.

Será de aplicación cuatro semanas después de su entrada en vigor.

Hecho en Bruselas, el 21 de marzo de 2022.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

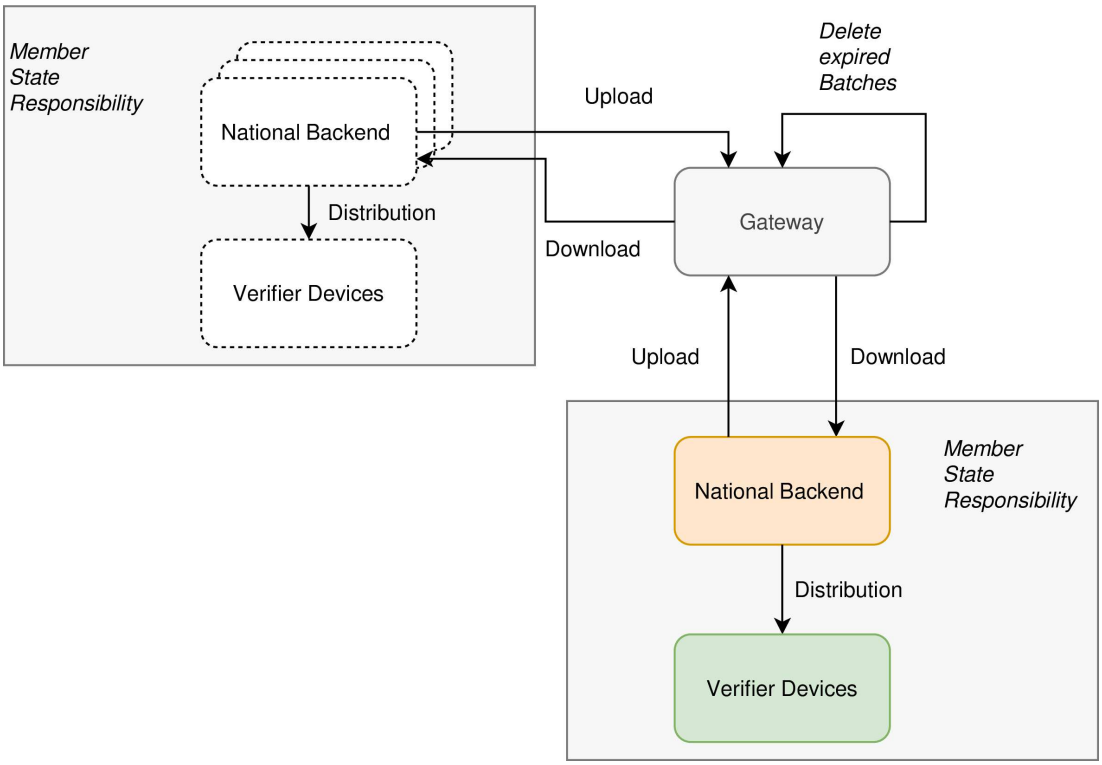
ANEXO I

Se añade la siguiente sección 9 en el anexo I de la Decisión de Ejecución (UE) 2021/1073:

«9. **SOLUCIÓN DE REVOCACIÓN**

9.1. **Disposición de la Lista de Revocación CCD (DLR)**

La pasarela proporcionará puntos de conexión y funcionalidad para alojar y gestionar las listas de revocación:



9.2. **Modelo de confianza**

Todas las conexiones se establecen mediante el modelo de confianza DCCG estándar mediante los certificados NB_{TLS} y NB_{UP} (véase la gobernanza de certificados). Toda la información se empaqueta y se carga mediante mensajes CMS para garantizar la integridad.

9.3. **Construcción de lotes**

9.3.1. *Lote*

Cada lista de revocación contendrá una o varias entradas y se empaquetará en lotes que contengan un conjunto de hashes y sus metadatos. Un lote es inmutable y define una fecha de caducidad que indica cuándo puede eliminarse el lote. La fecha de caducidad de todos los elementos del lote debe ser exactamente la misma, es decir, los lotes deben agruparse por fecha de caducidad y por DSC firmante. Cada lote contendrá un máximo de 1 000 entradas. Si la lista de revocación consta de más de 1 000 entradas, se crearán varios lotes. Una entrada determinada solo puede producirse, como máximo, en un lote. El lote se empaquetará en una estructura CMS y se firmará con el certificado NB_{up} del país que lo cargue.

9.3.2. *Índice de lotes*

Cuando se cree un lote, la pasarela le asignará un identificador único y se añadirá automáticamente al índice. El índice de lotes se ordenará por la fecha modificada, en orden cronológico ascendente.

9.3.3. *Comportamiento de la pasarela*

La pasarela procesa los lotes de revocación sin introducir cambios: no puede actualizar, eliminar ni añadir información a los lotes. Los lotes se envían a todos los países autorizados (véase el capítulo 9.6).

La pasarela controla activamente las fechas de caducidad de los lotes y elimina los lotes caducados. Después de eliminar el lote, la pasarela muestra la respuesta "HTTP 410 Gone" para la URL del lote eliminado. Así, el lote eliminado aparece como "deleted" en el Índice de lotes.

9.4. **Tipos de hash**

La lista de revocación contiene hashes que pueden representar diferentes tipos o atributos de revocación. Estos tipos o atributos se indicarán al confeccionarse las listas de revocación. Los tipos actuales son los siguientes:

Tipo	Atributo	Cálculo del hash
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (identificador único de certificado)	SHA256 of UCI
COUNTRYCODEUCI	Código del país emisor + UCI	SHA256 of Issuing CountryCode + UCI

Solo los primeros 128 bits de los hashes codificados como cadenas base64 se introducen en los lotes y se utilizan para identificar el CCD revocado ([1]).

9.4.1. *Tipo de hash: SHA-256(firma CCD)*

En este caso, el hash se calcula sobre los bytes de la firma COSE_SIGN1 del CWT. Para las firmas RSA se utilizará la firma completa como entrada. La fórmula de los certificados con firma EC-DSA utiliza el valor r como entrada:

SHA256(r)

[necesario para todas las nuevas implementaciones]

9.4.2. *Tipo de hash: SHA-256(UCI)*

En este caso, el hash se calcula sobre la cadena UCI codificada en UTF-8 y se convierte en una matriz de bytes (*byte array*).

[obsoleto ([2]), pero adecuado para la retrocompatibilidad]

9.4.3. *Tipo de hash: SHA256(Issuing CountryCode+UCI)*

En este caso, el CountryCode codificado como una cadena UTF-8 concatenada con la UCI codificada con una cadena UTF-8. Esto se convierte después en una matriz de bytes (*byte array)* y se utiliza como entrada para la función hash.

[obsoleto[2], pero adecuado para la retrocompatibilidad]

9.5. **Estructura API**

9.5.1. *API de suministro de las entradas de revocación*

9.5.1.1. Finalidad

El API proporciona las entradas de la lista de revocación en lotes, incluido un índice de lotes.

9.5.1.2. Puntos de conexión

([1]) Téngase en cuenta también el punto 9.5.1.2 para las descripciones detalladas de las API.
([2]) Obsoleto significa que esta función no se tendrá en cuenta para nuevas implementaciones, pero será compatible con implementaciones existentes durante un período de tiempo bien definido.

9.5.1.2.1. Punto de conexión para la descarga de listas de lotes.

Los puntos de conexión siguen un diseño sencillo y devuelven una lista de lotes con un pequeño contenedor (*wrapper*) que facilita los metadatos. Los lotes se clasifican por *fecha* en orden *(cronológico) ascendente*:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    'more':true|false,
    'batches':
        [{
            'batchId': '{uuid}',
            'country': 'XY',
            'date': '2021-11-01T00:00:00Z'
            'deleted': true | false
        }, ..
        ]
}
```

Nota: El resultado se limita por defecto a 1 000. Si la indicación "more" se establece como "true", la respuesta indica que hay más lotes disponibles para descargar. Para descargar más elementos, el cliente debe configurar el encabezado If-Modified-Since en una fecha no anterior a la última entrada recibida.

La respuesta contiene una matriz JSON con la siguiente estructura:

Campo	Definición
more	Indicador booleano que indica que hay más lotes.
batches	Matriz con los lotes existentes.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Código del país ISO 3166
date	ISO 8601 Date UTC. Fecha en que se añadió o eliminó el lote.
deleted	Valor booleano. "True" en caso que se elimine. Cuando se activa la marca "deleted" (eliminado), la entrada puede suprimirse definitivamente de los resultados de la consulta al cabo de 7 días.

9.5.1.2.1.1. *Códigos* de respuesta

Código	Descripción
200	Todo correcto.
204	Sin contenido, si el contenido del encabezado "If-Modified-Since" no tiene ninguna correspondencia.

Encabezado de solicitud

Encabezado	Obligatorio	Descripción
If-Modified-Since	Sí	Este encabezado contiene la última fecha descargada para obtener únicamente los resultados más recientes. En la llamada inicial, el encabezado debe seguir el formato '2021-06-01 T00:00:00Z'

9.5.1.2.2. Punto de conexión para descarga de lotes.

Los lotes contienen una lista de identificadores de certificado:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

'country': 'XY',

'expires': '2022-11-01T00:00:00Z',

'kid':'23S+33f=',

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

La respuesta contiene un CMS que incluye una firma que debe corresponder al certificado NB_{UP} del país. Todos los elementos de la matriz JSON tienen la siguiente estructura:

Campo	Obligatorio	Tipo	Definición
expires	Sí	Cadena	Fecha en que puede suprimirse el elemento. Fecha/hora UTC ISO8601
country	Sí	Cadena	Código del país ISO 3166
hashType	Sí	Cadena	Tipo de hash de las entradas facilitadas (véase "Tipos de hash)
entries	Sí	JSON Object Array	Véase el cuadro Entradas
kid	Sí	Cadena	KID codificado en Base64 del DSC utilizado para firmar el CCD. Si el KID no es conocido, se puede utilizar la cadena `UNKNOWN_KID` (sin `).

Notas:

— Los lotes se agruparán por fecha de caducidad y DSC: todos los elementos caducarán al mismo tiempo y habrán sido firmados por la misma clave.

— La hora de caducidad es una fecha/hora indicada en UTC, ya que el CCD de la UE es un sistema mundial y debemos utilizar una hora inequívoca.

— La fecha de expiración de un CCD revocado de forma permanente se fijará en la fecha de expiración del DSC correspondiente utilizado para firmar el CCD o en la hora de expiración del CCD revocado (en cuyo caso se considerará que las horas NumericDate/epoch utilizadas se encuentran en la zona horaria del UTC).

— El backend nacional (NB) suprimirá los elementos de su lista de revocación cuando se alcance la fecha de **caducidad**.

— El *Nota:* puede suprimir elementos de su lista de revocación en caso de que se revoque el **kid** utilizado para firmar el CCD.

9.5.1.2.2.1. Entradas

Campo	Obligatorio	Tipo	Definición
hash	Sí	Cadena	Primeros 128 bits del hash SHA-256 codificado como cadena de base64

Nota: El objeto de las entradas solo contiene actualmente un hash, pero, para ser compatible con cambios futuro, se eligió un objeto en lugar de una matriz JSON.

9.5.1.2.2.2. Códigos de respuesta

Código	Descripción
200	Todo correcto.
410	El lote ha desaparecido. Se puede eliminar el lote en el backend nacional.

9.5.1.2.2.3. Encabezados de respuesta

Encabezado	Descripción
ETag	ID del lote.

9.5.1.2.3. Punto de conexión para carga de lotes.

La carga se realiza sobre el mismo punto de conexión mediante el verbo (*verb*) POST:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

{

‘country’: ‘XY’,

‘expires’: ‘2022-11-01T00:00:00Z’,

‘kid’:’23S+33f=’,

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

El lote se firmará mediante el certificado NB_{UP}. La pasarela verificará que la firma se basa en el NB_{UP} para el *country* (país) en cuestión. Si el control de la firma es negativo, no se producirá la carga.

Nota: Cada lote es inmutable y no puede cambiarse después de cargarlo. Sin embargo, puede eliminarse. Se almacena el ID de cada lote eliminado y se rechaza la carga de un nuevo lote que tenga el mismo ID.

9.5.1.2.4. Punto de conexión para eliminación de lotes.

Un lote se puede eliminar en el mismo punto de conexión mediante el *Verb* DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

o, por razones de compatibilidad, al siguiente punto de conexión con el *Verb* POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

9.6. **Protección API/RGPD**

En esta sección se especifican las medidas necesarias para que la implementación cumpla con las disposiciones del Reglamento (CE) 2021/953 en lo que respecta al tratamiento de datos personales.

9.6.1. *Autenticación existente*

La pasarela utiliza actualmente el certificado NB_{TLS} para autenticar a los países que se conectan con la pasarela. Esta autenticación puede utilizarse para determinar la identidad del país conectado a la pasarela. Esta identidad puede utilizarse seguidamente para realizar el control de acceso.

9.6.2. *Control de acceso*

Para poder tratar legalmente datos personales, la pasarela aplicará un mecanismo de control de acceso.

La pasarela aplica una lista de control de acceso en combinación con una seguridad basada en roles. En dicho sistema se mantendrán dos cuadros: uno en el que se describan qué roles pueden aplicarse a qué operaciones sobre qué recursos, y otro en el que se describen qué roles se asignan a qué usuarios.

Para realizar los controles exigidos en el presente documento, se requieren tres roles, a saber:

RevocationListReader

RevocationUploader

RevocationDeleter

Los siguientes puntos de conexión comprobarán si el usuario tiene el rol RevocationListReader; en caso afirmativo se concederá el acceso; de lo contrario, aparecerá HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Los siguientes puntos de conexión comprobarán si el usuario tiene el rol RevocationUploader; en caso afirmativo se concederá el acceso; de lo contrario, aparecerá HTTP 403 Forbidden:

POST/revocation-list

Los siguientes puntos de conexión comprobarán si el usuario tiene el rol RevocationDeleter; en caso afirmativo se concederá el acceso; de lo contrario, aparecerá HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

La pasarela también proporcionará un método fiable mediante el cual los administradores puedan gestionar los roles vinculados a los usuarios de manera que se reduzcan las posibilidades de errores humanos sin que ello suponga una carga para los administradores funcionales.».

ANEXO II

La sección 3 del anexo V de la Decisión de Ejecución (UE) 2021/1073 se modifica como sigue:

«3. ***Estructuras comunes y requisitos generales***

No se expedirá un certificado COVID digital de la UE si no pueden cumplimentarse correctamente todos los campos de datos de conformidad con esta especificación debido a la falta de información. **Esto no se entenderá en el sentido de que afecta a la obligación de los Estados miembros de expedir certificados COVID digitales de la UE.**

La información de todos los campos puede facilitarse utilizando el conjunto completo de 13.0 caracteres de UNICODE codificados en UTF-8, a menos que se limite específicamente a conjuntos de valores o conjuntos de caracteres más reducidos.

La estructura común será la siguiente:

"JSON":{

"ver":<version information>,

"nam":{

<person name information>

},

"dob":<date of birth>,

"v" or "t" or "r":[

{<vaccination dose or test or recovery information, one entry>}

]

}

En las secciones siguientes se ofrece información detallada sobre los distintos grupos y campos.

Cuando las normas indiquen que debe omitirse un campo, esto significa que su contenido estará vacío y que no se permiten ni el nombre ni el valor del campo en el contenido.

3.1. ***Versión***

Se proporcionará información sobre la versión. La gestión de las versiones se realiza de acuerdo con el Semantic Versioning (semver: https://semver.org). En la producción, será una de las versiones publicadas oficialmente (la actual o una más antigua oficialmente publicada). Véase la sección JSON Schema location para más detalles.

ID del campo	Nombre del campo	Instructiones
ver	Versión del sistema	Coincidirá con el identificador de la versión del sistema utilizado para elaborar el CCD de la UE. Ejemplo: "ver":"1.3.0"

3.2. ***Nombre y fecha de nacimiento***

El nombre de la persona es el nombre oficial completo de la persona, que coincide con el nombre indicado en los documentos de viaje. El identificador de la estructura es *nam*. Se facilitará exactamente 1 (un) nombre de persona.

ID del campo	Nombre del campo	Instrucciones
nam/fn	Apellido(s)	Apellido(s) del titular Si el titular no tiene apellido(s) pero tiene nombre, se omitirá el campo. En el resto de los casos, se facilitará exactamente 1 (un) campo no vacío, con todos los apellidos incluidos en él. En caso de pluralidad de apellidos, estos estarán separados por un espacio. No obstante, los nombres combinados que incluyan guiones o caracteres similares deberán permanecer iguales.

		Ejemplos: “fn”:“Musterfrau-Gößinger” “fn”:“Musterfrau-Gößinger Müller”
nam/fnt	Apellido(s) normalizado(s)	Apellido(s) del titular transliterado(s) utilizando la misma convención que la aplicada en los documentos de viaje de lectura mecánica del titular (tales como las normas definidas en el documento 9303 de la OACI, parte 3). Si el titular no tiene apellido(s) pero tiene nombre, se omitirá el campo. Se facilitará exactamente 1 (un) campo no vacío, utilizando solo los caracteres A-Z y <. Longitud máxima: 80 caracteres (según la especificación de la OACI 9303). Ejemplos: “fnt”:“MUSTERFRAU<GOESSINGER” “fnt”:“MUSTERFRAU<GOESSINGER<MUELLER”
nam/gn	Nombre(s)	Nombre(s) del titular. Si el titular no tiene nombre(s) pero tiene apellido(s), se omitirá el campo. En el resto de los casos, se facilitará exactamente 1 (un) campo no vacío, con todos los nombres incluidos en él. En caso de pluralidad de nombres, estos estarán separados por un espacio. Ejemplo: “gn”:“Isolde Erika”
nam/gnt	Nombre(s) normalizado(s)	Nombres(s) del titular transliterado(s) utilizando la misma convención que la aplicada en los documentos de viaje de lectura mecánica del titular (tales como las normas definidas en el documento 9303, parte 3, de la OACI). Si el titular no tiene nombre pero tiene apellido(s), se omitirá el campo. Se facilitará exactamente 1 (un) campo no vacío, utilizando solo los caracteres A-Z y <. Longitud máxima: 80 caracteres Ejemplo: “gnt”:“ISOLDE<ERIKA”
dob	Fecha de nacimiento	Fecha de nacimiento del titular del CCD. Fecha completa o parcial sin indicación de tiempo limitada al intervalo de 1900-01-01 a 2099-12-31. Se facilitará exactamente 1 (un) campo no vacío si se conoce la fecha de nacimiento completa o parcial. Si la fecha de nacimiento no se conoce ni siquiera parcialmente, el campo lo constituirá una cadena vacía “”. Esta información debe coincidir con la facilitada en los documentos de viaje. Se utilizará uno de los siguientes formatos ISO 8601 si se dispone de información sobre la fecha de nacimiento. No se admiten otras opciones. AAAA-MM-DD AAAA-MM AAAA (La aplicación del verificador puede mostrar las partes de la fecha de nacimiento que faltan utilizando la convención XX, como la empleada en documentos de viaje de lectura mecánica, por ejemplo, 1990-XX-XX.) Ejemplos: “dob”:“1979-04-14” “dob”: “1901-08 ” “dob”:“1939” “dob”:

3.3. ***Grupos para la información específica sobre el tipo de certificado***

El sistema JSON admite tres grupos de entradas que incluyen información específica sobre el tipo de certificado. Cada CCD de la UE contendrá exactamente 1 (un) grupo. No se permiten grupos vacíos.

Identificador del grupo	**Nombre del grupo**	**Entradas**
v	Grupo de vacunación	Si fuera el caso, deberá contener exactamente 1 (una) entrada que indique exactamente 1 (una) dosis de vacunación (una dosis).
t	Grupo de prueba	Si fuera pertinente, deberá contener exactamente 1 (una) entrada que indique exactamente 1 (un) resultado de una prueba.
r	Grupo de recuperación	Si fuera pertinente, deberá contener exactamente 1 (una) entrada que indique 1 (un) certificado de recuperación.».

ANEXO III

«ANEXO VI

RESPONSABILIDADES DE LOS ESTADOS MIEMBROS COMO CORRESPONSABLES DEL TRATAMIENTO DE LA PASARELA DEL CERTIFICADO COVID DIGITAL DE LA UE PARA EL INTERCAMBIO DE LISTAS DE REVOCACIÓN DEL CCD DE LA UE

SECCIÓN 1

Subsección 1

División de responsabilidades

1) Los corresponsables del tratamiento tratarán los datos personales a través de la pasarela del marco de confianza de conformidad con las especificaciones técnicas del anexo I.

2) Las autoridades expedidoras de los Estados miembros siguen siendo las únicas responsables de la recogida, el uso, la divulgación y cualquier otro tratamiento de la información relativa a la revocación fuera del portal, incluido el procedimiento que condujo a la revocación de un certificado.

3) Cada responsable del tratamiento de los datos personales en la pasarela del marco de confianza lo será de conformidad con los artículos 5, 24 y 26 del Reglamento general de protección de datos.

4) Cada responsable del tratamiento establecerá un punto de contacto con un buzón funcional que servirá para la comunicación entre los propios corresponsables y entre estos y el encargado del tratamiento.

5) Se encomendará a un grupo de trabajo creado por el Comité a que se refiere el artículo 14 del Reglamento (UE) 2021/953 la tarea de tomar decisiones sobre cualquier cuestión que surja del intercambio de listas de revocación y de la corresponsabilidad del tratamiento de datos personales correspondiente y de facilitar instrucciones coordinadas a la Comisión como encargada del tratamiento. El proceso de toma de decisiones de los corresponsables del tratamiento se rige por dicho grupo de trabajo y por el reglamento interno que debe adoptar. Como regla de base, la ausencia de cualquiera de los corresponsables del tratamiento en una reunión de este grupo de trabajo, que haya sido anunciada con al menos siete (7) días de antelación a su convocatoria por escrito, conlleva el consentimiento tácito a lo acordado en la misma. Cualquiera de los corresponsables del tratamiento puede convocar una reunión de este grupo de trabajo.

6) Las instrucciones dirigidas al encargado del tratamiento serán enviadas por cualquiera de los puntos de contacto de los corresponsables del tratamiento, de acuerdo con los demás corresponsables, según el proceso de toma de decisiones del grupo de trabajo descrito en el punto 5 anterior. El corresponsable del tratamiento que proporcione las instrucciones debe facilitarlas por escrito al encargado del tratamiento e informar de ello a todos los demás corresponsables del tratamiento. Si el asunto en cuestión es tan urgente que no permite una reunión del grupo de trabajo como se menciona en el punto 5 anterior, se puede proporcionar una instrucción de todos modos, pero el grupo de trabajo puede rescindirla. Esta instrucción debe ser comunicada por escrito, y todos los demás corresponsables del tratamiento deben ser informados de esto en el momento de su comunicación.

7) El grupo de trabajo establecido según lo dispuesto en el punto 5 anterior no excluye la competencia individual de ninguno de los corresponsables del tratamiento para informar a su autoridad de supervisión competente de conformidad con los artículos 33 y 24 del Reglamento general de protección de datos. Dicha notificación no requiere el consentimiento de ninguno de los demás corresponsables del tratamiento.

8) En el ámbito de aplicación de la pasarela del marco de confianza, solo podrán acceder a los datos personales intercambiados las personas autorizadas por las autoridades nacionales o los organismos oficiales designados.

9) Cada autoridad expedidora llevará un registro de las actividades de tratamiento bajo su responsabilidad. La corresponsabilidad podrá indicarse en dicho registro.

Subsección 2

Responsabilidades y funciones para la tramitación de las solicitudes de los interesados y la información a estos

1) Cada responsable del tratamiento, en su calidad de autoridad expedidora, facilitará a las personas físicas cuyo certificado o certificados haya revocado ("interesados") información relativa a dicha revocación y al tratamiento de sus datos personales en la pasarela del certificado COVID digital de la UE a efectos de apoyar el intercambio de listas de revocación, de conformidad con el artículo 14 del Reglamento general de protección de datos, a menos que ello resulte imposible o suponga un esfuerzo desproporcionado.

2) Cada responsable del tratamiento actuará como punto de contacto para las personas físicas cuyo certificado haya revocado y tramitará las solicitudes presentadas por los interesados o sus representantes en el ejercicio de sus derechos de conformidad con el Reglamento general de protección de datos. Si un corresponsable del tratamiento recibe una solicitud de un interesado relativa a un certificado expedido por otro corresponsable del tratamiento, informará al interesado de la identidad y datos de contacto de dicho corresponsable del tratamiento. Si así lo solicita otro corresponsable del tratamiento, estos se ayudarán mutuamente en la tramitación de las solicitudes de los interesados y se responderán sin demora excesiva y, a más tardar, en el plazo de un mes desde la recepción de la solicitud de ayuda. Si una solicitud está relacionada con datos presentados por un tercer país, el responsable del tratamiento que reciba la solicitud la tramitará e informará al interesado de la identidad y datos de contacto de la autoridad expedidora del tercer país.

3) Cada responsable del tratamiento pondrá a disposición de los interesados el contenido del presente anexo, en especial las disposiciones establecidas en los puntos 1 y 2.

SECCIÓN 2

Gestión de los incidentes de seguridad, especialmente las violaciones de la seguridad de los datos personales

1) Los corresponsables del tratamiento se ayudarán mutuamente en la detección y el manejo de los incidentes de seguridad, especialmente las violaciones de la seguridad de los datos personales, relacionados con el tratamiento en la pasarela del certificado COVID digital de la UE.

2) En particular, los corresponsables del tratamiento se notificarán lo siguiente:

   a) todo riesgo potencial o real para la disponibilidad, confidencialidad o integridad de los datos personales objeto de tratamiento en la pasarela del marco de confianza;

   b) toda violación de la seguridad de los datos personales, sus consecuencias probables y la evaluación del riesgo con respecto a los derechos y libertades de las personas físicas, así como toda medida adoptada para resolver dicha violación y mitigar dicho riesgo;

   c) todo incumplimiento de las salvaguardas técnicas u organizativas de la operación de tratamiento en la pasarela del marco de confianza.

3) Los corresponsables del tratamiento comunicarán toda violación de la seguridad de los datos personales relacionada con la operación de tratamiento en la pasarela del marco de confianza a la Comisión a las autoridades de control competentes y, en su caso, a los interesados, de conformidad con los artículos 33 y 34 del Reglamento general de protección de datos o tras la notificación de la Comisión.

4) Cada autoridad expedidora aplicará las medidas técnicas y organizativas adecuadas, destinadas a:

   a) garantizar y proteger la disponibilidad, integridad y confidencialidad de los datos personales tratados conjuntamente;

   b) proteger los datos personales que obren en su poder contra todo tratamiento, pérdida, utilización, divulgación, adquisición o acceso no autorizados o ilícitos;

   c) garantizar que el acceso a los datos personales no se comunique ni se permita a ninguna persona distinta de los destinatarios o encargados del tratamiento.

SECCIÓN 3

Evaluación de impacto relativa a la protección de datos

1) Si un responsable del tratamiento, para cumplir las obligaciones que le imponen los artículos 35 y 36 del Reglamento (UE) 2016/679, necesita información de otro responsable del tratamiento, enviará una solicitud específica al buzón funcional al que se refiere la sección 1, subsección 1, punto 4. Este último responsable hará lo posible por facilitar esa información.».

ANEXO IV

«ANEXO VII

RESPONSABILIDADES DE LA COMISIÓN COMO ENCARGADA DEL TRATAMIENTO DE DATOS EN LA PASARELA DEL CERTIFICADO COVID DIGITAL DE LA UE PARA EL INTERCAMBIO DE LISTAS DE REVOCACIÓN DEL CCD DE LA UE

La Comisión deberá:

1) Crear y garantizar una infraestructura de comunicación segura y fiable en nombre de los Estados miembros que permita el intercambio de listas de revocación presentadas en la pasarela del certificado COVID digital de la UE.

2) Para cumplir sus obligaciones como encargada del tratamiento de datos del portal del marco de confianza para los Estados miembros, la Comisión podrá recurrir a terceros como subencargados del tratamiento; La Comisión informará a los corresponsables del tratamiento de cualquier cambio previsto en relación con la adición o sustitución de otros subencargados del tratamiento, dándoles así la oportunidad de oponerse de forma conjunta a tales cambios. Asimismo, deberá velar por que se apliquen a estos subencargados del tratamiento las mismas obligaciones de protección de datos que contiene la presente Decisión.

3) Tratar los datos personales basándose exclusivamente en las instrucciones documentadas dadas por los responsables del tratamiento, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros; en tal caso, la Comisión informará a los responsables del tratamiento de ese requisito jurídico antes del tratamiento, a menos que el citado Derecho prohíba enviar esa información por motivos importantes de interés público.

   El tratamiento por parte de la Comisión conlleva lo siguiente:

   a) la autenticación de los servidores finales nacionales, basada en los certificados de estos;

   b) la recepción de los datos a los que se refiere el artículo 5 bis, apartado 3, de la Decisión, cargados por los servidores finales nacionales mediante una interfaz de programación de aplicaciones que les permite cargar los datos pertinentes;

   c) el almacenamiento de los datos en la pasarela del certificado COVID digital de la UE;

   d) la disposición de los datos de modo que puedan ser descargados por los servidores finales nacionales;

   e) la supresión de los datos en su fecha de expiración o por orden del responsable del tratamiento que los haya presentado;

   f) al finalizar la prestación del servicio, la eliminación de los datos restantes, salvo que el Derecho de la Unión o del Estado miembro exija el almacenamiento de los datos personales.

4) Adoptar todas las medidas de seguridad organizativa, física y lógica más avanzadas que sean necesarias para el mantenimiento de la pasarela del certificado COVID digital de la UE. A tal fin, la Comisión deberá:

   a) designar una entidad responsable de la gestión de la seguridad en la pasarela del certificado COVID digital de la UE, comunicar a los corresponsables del tratamiento sus datos de contacto y garantizar su disponibilidad para reaccionar ante las amenazas para la seguridad;

   b) asumir la responsabilidad respecto a la seguridad de la pasarela del certificado COVID digital de la UE, incluyendo la realización periódica de pruebas, evaluaciones y valoraciones de las medidas de seguridad;

   c) velar por que todas las personas a las que se conceda acceso a la pasarela del certificado COVID digital de la UE estén sujetas a una obligación contractual, profesional o legal de confidencialidad.

5) Adoptar todas las medidas de seguridad necesarias para evitar comprometer el correcto funcionamiento operativo de los servidores finales nacionales. A tal fin, instaurará procedimientos específicos relativos a la conexión de los servidores finales con la pasarela del certificado COVID digital de la UE. Esto incluye:

   a) un procedimiento de evaluación de riesgos a fin de detectar y estimar las amenazas potenciales para el sistema;

   b) un procedimiento de auditoría y verificación a fin de:

      i) comprobar la correspondencia entre las medidas de seguridad implementadas y la política de seguridad aplicable,

      ii) controlar periódicamente la integridad de los ficheros del sistema, los parámetros de seguridad y las autorizaciones concedidas,

iii) vigilar para detectar violaciones de la seguridad e intrusiones,

iv) introducir cambios para mitigar las deficiencias existentes en materia de seguridad,

v) definir las condiciones en las que se autorizará, también a petición de los responsables del tratamiento, la realización de auditorías independientes, en particular inspecciones, y verificaciones de las medidas de seguridad, y se contribuirá a ellas, sujeto a condiciones que respeten el Protocolo (n.º 7) del TFUE sobre los privilegios e inmunidades de la Unión Europea;

c) la modificación del procedimiento de control para documentar y medir el impacto de un cambio antes de aplicarlo y la información continua a los responsables del tratamiento sobre los cambios que puedan afectar a la comunicación con sus infraestructuras o a la seguridad de estas,

d) el establecimiento de un procedimiento de mantenimiento y reparación para especificar las normas y condiciones que han de respetarse cuando deba procederse al mantenimiento o la reparación de equipos,

e) el establecimiento de un procedimiento en caso de incidentes de seguridad para definir el régimen de notificación y remisión a instancia superior, informar sin demora a los responsables correspondientes del tratamiento para que notifiquen a las autoridades nacionales de supervisión de la protección de datos cualquier violación de la seguridad de los datos personales y definir un procedimiento disciplinario para las violaciones de la seguridad.

6) Adoptar las medidas de seguridad física o lógica más avanzadas para las instalaciones que alojen el equipo de la pasarela del certificado COVID digital de la UE y para los controles de los datos lógicos y el acceso de seguridad. A tal fin, la Comisión deberá:

a) poner en ejecución medidas de seguridad física a fin de establecer perímetros de seguridad nítidos que permitan detectar las violaciones;

b) controlar el acceso a las instalaciones y mantener un registro de visitantes a efectos de seguimiento;

c) velar por que las personas externas a las que se haya concedido acceso a los locales sean acompañadas por personal debidamente autorizado;

d) velar por que no puedan añadirse, sustituirse ni retirarse equipos sin la autorización previa de los organismos responsables designados;

e) controlar el acceso desde y hacia los servidores finales nacionales en la pasarela del marco de confianza;

f) velar por que las personas que accedan a la pasarela del certificado COVID digital de la UE estén identificadas y autenticadas;

g) verificar los derechos de autorización relacionados con el acceso a la pasarela del certificado COVID digital de la UE en caso de que se produzca una violación de la seguridad que afecte a esta infraestructura;

h) mantener la integridad de la información transmitida a través de la pasarela del certificado COVID digital de la UE;

i) aplicar medidas de seguridad técnica y organizativa para evitar el acceso no autorizado a datos personales;

j) aplicar, siempre que sea necesario, medidas para bloquear el acceso no autorizado a la pasarela del certificado COVID digital de la UE desde el dominio de las autoridades expedidoras (es decir: bloqueo de una ubicación o de una dirección IP).

7) Adoptar medidas para proteger su dominio, incluida la desconexión, en caso de que se produzca una desviación sustancial con respecto a los principios y conceptos de calidad o seguridad.

8) Mantener un plan de gestión de riesgos relacionado con su ámbito de responsabilidad.

9) Monitorizar, en tiempo real, el funcionamiento de todos los componentes de servicio de sus servicios de la pasarela del marco de confianza, elaborar estadísticas regulares y llevar registros.

10) Prestar apoyo con respecto a todos los servicios de la pasarela del marco de confianza en inglés, las veinticuatro horas del día, siete días a la semana, por teléfono, correo electrónico o portal web, y aceptar las llamadas de los usuarios autorizados: los coordinadores de la pasarela del Certificado COVID Digital de la UE y sus respectivos servicios de asistencia, responsables de proyectos y personas designadas por la Comisión.

11) Ayudar en la medida de lo posible a los responsables del tratamiento con medidas técnicas y organizativas apropiadas de conformidad con el artículo 12 del Reglamento (UE) 2018/1725 para que cumplan su obligación de responder a las solicitudes de ejercicio de los derechos de los interesados establecidas en el capítulo III del Reglamento general de protección de datos.

12) Ayudar a los corresponsables del tratamiento proporcionándoles información sobre la pasarela del Certificado COVID Digital de la UE, a fin de dar cumplimiento a las obligaciones derivadas de los artículos 32, 33, 34, 35 y 36 del Reglamento general de protección de datos;

13) Garantizar que los datos tratados en la pasarela del Certificado COVID Digital de la UE sean ininteligibles para cualquier persona que no esté autorizada a acceder a ella;

14) Adoptar todas las medidas pertinentes para impedir que los operadores de la pasarela del Certificado COVID Digital de la UE accedan sin autorización a los datos transmitidos;

15) Adoptar medidas para facilitar la interoperabilidad y la comunicación entre los responsables del tratamiento designados de la pasarela del Certificado COVID Digital de la UE;

16) Llevar un registro de las actividades de tratamiento realizadas en nombre de los corresponsables del tratamiento de conformidad con el artículo 31, apartado 2, del Reglamento (UE) 2018/1725.».