II

(Actos no legislativos)

DECISIONES

DECISIÓN DE EJECUCIÓN (UE) 2020/1023 DE LA COMISIÓN

de 15 de julio de 2020

que modifica la Decisión de Ejecución (UE) 2019/1765 en lo concerniente al intercambio transfronterizo de datos entre las aplicaciones móviles nacionales de rastreo de contactos y advertencia para combatir la pandemia de COVID-19

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Vista la 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 ([1]), y en particular su artículo 14, apartado 3,

Considerando lo siguiente:

(1) De acuerdo con el artículo 14 de la Directiva 2011/24/UE, la Unión debe apoyar y facilitar la cooperación y el intercambio de información entre los Estados miembros dentro de una red voluntaria que conecte a las autoridades nacionales encargadas de la sanidad electrónica («la red de sanidad electrónica») designadas por los Estados miembros.

(2) La Decisión de Ejecución (UE) 2019/1765 de la Comisión ([2]) establece las normas del establecimiento, la gestión y el funcionamiento de la red de autoridades nacionales encargadas de la sanidad electrónica. El artículo 4 de dicha Decisión confía a la red de sanidad electrónica la tarea de facilitar una mayor interoperabilidad de los sistemas nacionales de tecnologías de la información y de las comunicaciones y la transferibilidad transfronteriza de los datos sanitarios electrónicos en la asistencia sanitaria transfronteriza;

(3) A la luz de la crisis de salud pública provocada por la pandemia de COVID-19, varios Estados miembros han desarrollado aplicaciones móviles que facilitan el rastreo de contactos y permiten advertir a sus usuarios para que tomen las medidas adecuadas, tales como someterse a pruebas o autoaislamiento, si han estado potencialmente expuestos al virus por haberse encontrado cerca de otro usuario de esas aplicaciones que ha informado de su diagnóstico positivo. Estas aplicaciones se basan en la tecnología Bluetooth para detectar la proximidad entre dispositivos. Dado que desde junio de 2020 se han ido suprimiendo las restricciones a los viajes entre Estados miembros, debe lograrse una mayor interoperabilidad de los sistemas nacionales de tecnologías de la información y de las comunicaciones entre los Estados miembros dentro de la red de sanidad electrónica, mediante la implantación de una infraestructura digital que permita la interoperabilidad entre las aplicaciones móviles nacionales que facilitan el rastreo de contactos y la advertencia.

([1]) DO L 88 de 4.4.2011, p. 45.

([2]) Decisión de Ejecución (UE) 2019/1765 de la Comisión, de 22 de octubre de 2019, por la que se establecen las normas del establecimiento, la gestión y el funcionamiento de la red de autoridades nacionales responsables en materia de sanidad electrónica y se deroga la Decisión de Ejecución 2011/890/UE (DO L 270 de 24.10.2019, p. 83).

(4) La Comisión ha estado prestando apoyo a los Estados miembros en relación con las aplicaciones móviles mencionadas. El 8 de abril de 2020, la Comisión adoptó una Recomendación relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados («la Recomendación de la Comisión») ([3]). Los Estados miembros de la red de sanidad electrónica adoptaron, con el apoyo de la Comisión, un conjunto de instrumentos comunes de la UE para los Estados miembros en relación con las aplicaciones móviles que facilitan el rastreo de contactos ([4]), así como directrices de interoperabilidad para las aplicaciones móviles de rastreo de contactos aprobadas en la UE ([5]). El conjunto de instrumentos explica los requisitos nacionales que han de cumplir las aplicaciones móviles nacionales de rastreo de contactos y advertencia, en particular que han de ser voluntarias, estar aprobadas por la autoridad sanitaria nacional correspondiente, preservar la privacidad y desmantelarse tan pronto como dejen de ser necesarias. Tras los últimos acontecimientos relacionados con la crisis de la COVID-19, tanto la Comisión ([6]) como el Comité Europeo de Protección de Datos ([7]) han publicado una serie de orientaciones sobre las aplicaciones móviles y las herramientas de rastreo de contactos, en lo referente a la protección de datos. El diseño de las aplicaciones móviles de los Estados miembros y de la infraestructura digital que permita su interoperabilidad se basa en el conjunto de instrumentos comunes de la UE, en las orientaciones mencionadas y en las especificaciones técnicas acordadas en el seno de la red de sanidad electrónica.

(5) Para facilitar la interoperabilidad de las aplicaciones móviles nacionales de rastreo de contactos y advertencia, los Estados miembros participantes en la red de sanidad electrónica que han decidido avanzar voluntariamente en su cooperación en este ámbito han desarrollado, con el apoyo de la Comisión, una infraestructura digital como herramienta informática para el intercambio de datos. Esta infraestructura digital se denomina «pasarela federativa» (*federation gateway*).

(6) La presente Decisión establece disposiciones sobre el papel de los Estados miembros participantes y de la Comisión en relación con el funcionamiento de la pasarela federativa para la interoperabilidad transfronteriza de las aplicaciones móviles nacionales de rastreo de contactos y advertencia.

(7) El tratamiento de los datos personales de los usuarios de las aplicaciones de rastreo de contactos y advertencia 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 ([8]) («el Reglamento general de protección de datos») y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([9]). El tratamiento de datos personales bajo la responsabilidad de la Comisión con el fin de gestionar y garantizar la seguridad de la pasarela federativa debe cumplir lo dispuesto en el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([10]).

(8) La pasarela federativa debe consistir en una infraestructura informática segura que proporcione una interfaz común, en la que las autoridades nacionales designadas o los organismos oficiales designados puedan intercambiar un conjunto mínimo de datos en relación con los contactos con personas infectadas por el SARS-CoV-2, a fin de informar a otras personas sobre su posible exposición a dicha infección y de promover una cooperación eficaz entre los Estados miembros en materia de asistencia sanitaria, facilitando el intercambio de la información pertinente.

(9) Por consiguiente, la presente Decisión debe establecer modalidades para el intercambio transfronterizo de datos dentro de la UE, a través de la pasarela federativa, entre las autoridades nacionales designadas o los organismos oficiales designados.

([3]) Recomendación (UE) 2020/518 de la Comisión, de 8 de abril de 2020, relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados (DO L 114 de 14.4.2020, p. 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

([6]) Comunicación de la Comisión «Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos» (DO C 124 I de 17.4.2020, p. 1).

([7]) Directrices 04/2020, sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, y declaración del CEPD de 16 de junio de 2020, sobre los efectos de la interoperabilidad de las aplicaciones de rastreo de contactos en la protección de datos, disponibles en: https://edpb.europa.eu

([8]) 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).

([9]) 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).

([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).

(10) Los Estados miembros participantes, representados por las autoridades nacionales designadas o los organismos oficiales designados, determinan conjuntamente el propósito y los medios de tratamiento de los datos personales a través de la pasarela federativa, por lo que son corresponsables del tratamiento. El artículo 26 del Reglamento general de protección de datos 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 sean determinadas por el Derecho de la Unión o del Estado miembro a que estén sujetos los responsables del tratamiento. Cada uno de los responsables del tratamiento debe garantizar que tiene una base jurídica a nivel nacional para efectuar el tratamiento en la pasarela federativa.

(11) La Comisión, como proveedora de soluciones técnicas y organizativas de la pasarela federativa, trata los datos personales seudonimizados en nombre de los Estados miembros participantes como corresponsables en la pasarela federativa y es, por lo tanto, una encargada del tratamiento. Según el artículo 28 del Reglamento general de protección de datos y el artículo 29 del Reglamento (UE) 2018/1725, 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 del tratamiento y que especifique el tratamiento. La presente Decisión expone las normas que rigen el tratamiento efectuado por la Comisión como encargada del tratamiento.

(12) Al tratar datos personales en el marco de la pasarela federativa, la Comisión debe atenerse a lo dispuesto en su Decisión (UE, Euratom) 2017/46 ([11]).

(13) Teniendo en cuenta que los fines para los que los responsables del tratamiento tratan los datos personales en las aplicaciones móviles de rastreo de contactos y advertencia no requieren necesariamente la identificación de un interesado, los responsables pueden no estar siempre en condiciones de garantizar la aplicación de los derechos de los interesados. En consecuencia, los derechos a los que se refieren los artículos 15 a 20 del Reglamento general de protección de datos pueden no ser de aplicación cuando se cumplan las condiciones establecidas en el artículo 11 de dicho Reglamento.

(14) El actual anexo de la Decisión de Ejecución (UE) 2019/1765 debe volver a numerarse, debido a la adición de dos nuevos anexos.

(15) Procede, por tanto, modificar la Decisión de Ejecución (UE) 2019/1765 en consecuencia.

(16) Considerando la urgencia de la situación provocada por la pandemia de COVID-19, la presente Decisión debe ser aplicable a partir del día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

(17) 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 9 de julio de 2020.

(18) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité creado conforme al artículo 16 de la Directiva 2011/24/UE.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

La Decisión de Ejecución (UE) 2019/1765 se modifica como sigue:

1) En el artículo 2, apartado 1, se insertan las letras g), h), i), j), k), l), m), n) y o) siguientes:

«g) "usuario de la aplicación": la persona en posesión de un dispositivo inteligente que ha descargado y ejecuta una aplicación móvil autorizada de rastreo de contactos y advertencia;

h) "rastreo de contactos" o "localización de contactos": las medidas aplicadas para seguir el rastro de las personas que han estado expuestas a una fuente de amenaza transfronteriza grave para la salud, en el sentido del artículo 3, letra c), de la Decisión n.º 1082/2013/UE del Parlamento Europeo y del Consejo (*);

([11]) Decisión (UE, Euratom) 2017/46, de 10 de enero de 2017, sobre la seguridad de los sistemas de información y comunicación de la Comisión Europea (DO L 6 de 11.1.2017, p. 40). 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

i) "aplicación móvil nacional de rastreo de contactos y advertencia": una aplicación informática aprobada a nivel nacional que funciona en dispositivos inteligentes, en particular teléfonos inteligentes, está normalmente diseñada para una interacción específica y de amplio alcance con recursos web y trata datos de proximidad y otra información contextual recogida por muchos de los sensores que se encuentran en los dispositivos inteligentes, con el fin de rastrear los contactos con personas infectadas por el SARS-CoV-2 y de advertir a las personas que pueden haber estado expuestas al SARS-CoV-2; estas aplicaciones móviles pueden detectar la presencia de otros dispositivos que utilizan Bluetooth e intercambiar información con servidores finales (*back-end*) a través de internet;

j) "pasarela federativa": la pasarela de red gestionada por la Comisión a través de una herramienta informática segura que recibe, almacena y pone a disposición de los servidores finales de los Estados miembros un conjunto mínimo de datos personales con el fin de garantizar la interoperabilidad de las aplicaciones móviles nacionales de rastreo de contactos y advertencia;

k) "clave": el identificador efímero único relacionado con un usuario de la aplicación que informa de que está infectado por el SARS-CoV-2, o de que puede haber estado expuesto al SARS-CoV-2;

l) "verificación de la infección": el método aplicado para confirmar una infección por SARS-CoV-2, a saber, si ha sido el propio usuario de la aplicación quien ha informado de la infección o si esta ha sido confirmada por una autoridad sanitaria nacional o una prueba de laboratorio;

m) "países de interés": los Estados miembros en los que ha estado un usuario de la aplicación en los catorce días previos a la fecha de carga de las claves y donde ha descargado la aplicación móvil nacional autorizada de rastreo de contactos y advertencia o ha estado de viaje;

n) "país de origen de las claves": el Estado miembro donde se encuentra el servidor final que cargó las claves en la pasarela federativa;

o) "datos de registro": el registro automático de una actividad relacionada con el intercambio de datos tratados a través de la pasarela federativa y con el acceso a dichos datos, que muestra, en particular, el tipo de actividad de tratamiento, la fecha y la hora de la actividad de tratamiento y el identificador de la persona que trata los datos.

(*) 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.º 2119/98/CE (DO L 293 de 5.11.2013, p. 1).».

2) En el artículo 4, apartado 1, se inserta la letra h) siguiente:

«h) proporcionar orientación a los Estados miembros sobre el intercambio transfronterizo de datos personales a través de la pasarela federativa entre las aplicaciones móviles nacionales de rastreo de contactos y advertencia.».

3) En el artículo 6, apartado 1, se insertan las letras f) y g) siguientes:

«f) desarrollará, instaurará y mantendrá las medidas técnicas y organizativas apropiadas en relación con la seguridad de la transmisión y el alojamiento de los datos personales en la pasarela federativa, a fin de garantizar la interoperabilidad de las aplicaciones móviles nacionales de rastreo de contactos y advertencia;

g) prestará apoyo a la red de sanidad electrónica a la hora de acordar la conformidad técnica y organizativa de las autoridades nacionales con los requisitos para el intercambio transfronterizo de datos personales en la pasarela federativa, proporcionando y llevando a cabo las pruebas y auditorías necesarias; los expertos de los Estados miembros podrán ayudar a los auditores de la Comisión.».

4) El artículo 7 se modifica como sigue:

a) el título se sustituye por «Protección de datos personales tratados a través de la infraestructura de servicios digitales de sanidad electrónica»;

b) en el apartado 2, el texto «anexo» se sustituye por el texto «anexo I».

5) Se inserta el artículo 7 *bis* siguiente:

«*Artículo 7 bis*

Intercambio transfronterizo de datos entre las aplicaciones móviles nacionales de rastreo de contactos y advertencia a través de la pasarela federativa

1. Cuando se intercambien datos personales a través de la pasarela federativa, el tratamiento se limitará a lo necesario para facilitar la interoperabilidad de las aplicaciones móviles nacionales de rastreo de contactos y advertencia dentro de la pasarela federativa y para permitir la continuidad del rastreo de contactos en un contexto transfronterizo.

2. Los datos personales a los que se refiere el apartado 3 se transmitirán a la pasarela federativa en formato seudonimizado.

3. Los datos personales seudonimizados intercambiados a través de la pasarela federativa y tratados en ella comprenderán únicamente la siguiente información:

a) las claves transmitidas por las aplicaciones móviles nacionales de rastreo de contactos y advertencia hasta catorce días antes de la fecha de carga de las claves;

b) los datos de registro asociados a las claves, en consonancia con el protocolo de especificaciones técnicas utilizado en el país de origen de las claves;

c) la verificación de la infección;

d) los países de interés y el país de origen de las claves.

4. Las autoridades nacionales designadas o los organismos oficiales designados que traten datos personales en la pasarela federativa serán corresponsables de los datos tratados en ella. Las respectivas responsabilidades de los corresponsables del tratamiento se asignarán de acuerdo con el anexo II. Todo Estado miembro que desee participar en el intercambio transfronterizo de datos entre las aplicaciones móviles nacionales de rastreo de contactos y advertencia deberá notificar previamente su intención a la Comisión e indicar la autoridad nacional o el organismo oficial que haya designado como responsable del tratamiento.

5. La Comisión será la encargada del tratamiento de los datos personales tratados dentro de la pasarela federativa. En su calidad de encargada del tratamiento, la Comisión deberá garantizar la seguridad del tratamiento, incluidos la transmisión y el alojamiento, de los datos personales dentro de la pasarela federativa y cumplir las obligaciones de los encargados del tratamiento establecidas en el anexo III.

6. La Comisión y las autoridades nacionales autorizadas a acceder a la pasarela federativa pondrán a prueba, examinarán y evaluarán periódicamente la eficacia de las medidas técnicas y organizativas destinadas a garantizar la seguridad del tratamiento de los datos personales dentro de la pasarela federativa.

7. Sin perjuicio de la decisión de los corresponsables del tratamiento de poner término al tratamiento dentro de la pasarela federativa, el funcionamiento de esta se desactivará, a más tardar, catorce días después de que todas las aplicaciones móviles nacionales de rastreo de contactos y advertencia conectadas dejen de transmitir claves a través de la pasarela federativa.».

6) El anexo pasa a ser el anexo I.

7) Se añaden los anexos II y III, cuyo texto figura en el anexo de la presente Decisión.

Artículo 2

La presente Decisión entrará en vigor el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 15 de julio de 2020.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

En la Decisión de Ejecución (UE) 2019/1765 se añaden los anexos II y III siguientes:

«*ANEXO II*

RESPONSABILIDADES DE LOS ESTADOS MIEMBROS PARTICIPANTES COMO CORRESPONSABLES DEL TRATAMIENTO EN LA PASARELA FEDERATIVA PARA EL TRATAMIENTO TRANSFRONTERIZO DE DATOS ENTRE LAS APLICACIONES MÓVILES NACIONALES DE RASTREO DE CONTACTOS Y ADVERTENCIA

SECCIÓN 1

Subsección 1

División de responsabilidades

1) Los corresponsables del tratamiento tratarán los datos personales a través de la pasarela federativa de conformidad con las especificaciones técnicas establecidas por la red de sanidad electrónica ([1]).

2) Cada responsable del tratamiento lo será respecto a los datos personales en la pasarela federativa de conformidad con el Reglamento general de protección de datos y con la Directiva 2002/58/CE.

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

4) Se encomendará a un subgrupo temporal creado por la red de sanidad electrónica de conformidad con el artículo 5, apartado 4, la tarea de examinar cualquier cuestión que surja en relación con la interoperabilidad de las aplicaciones móviles nacionales de rastreo de contactos y advertencia y con la corresponsabilidad del tratamiento de datos personales relacionado, y de facilitar instrucciones coordinadas a la Comisión en su calidad de encargada del tratamiento. Entre otras cuestiones, los responsables del tratamiento pueden trabajar, en el marco del subgrupo temporal, en busca de un enfoque común sobre la retención de los datos en sus servidores finales nacionales, teniendo en cuenta el período de retención indicado en la pasarela federativa.

5) 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 del subgrupo mencionado anteriormente.

6) Solo las personas autorizadas por las autoridades nacionales designadas o los organismos oficiales designados podrán acceder a los datos personales de los usuarios intercambiados en la pasarela federativa.

7) Cada autoridad nacional u organismo oficial designados dejarán de ser corresponsables del tratamiento desde la fecha en que se retiren de la pasarela federativa. Sin embargo, seguirán siendo responsables con respecto al tratamiento realizado en la pasarela federativa antes de su retirada.

Subsección 2

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

1) Cada responsable del tratamiento facilitará a los usuarios de su aplicación móvil nacional de rastreo de contactos y advertencia ("los interesados") información sobre el tratamiento de sus datos personales en la pasarela federativa a efectos de la interoperabilidad transfronteriza de las aplicaciones móviles nacionales de rastreo de contactos y advertencia, de conformidad con los artículos 13 y 14 del Reglamento general de protección de datos.

2) Cada responsable del tratamiento actuará como punto de contacto para los usuarios de su aplicación móvil nacional de rastreo de contactos y advertencia y tramitará las solicitudes relativas al ejercicio de los derechos de los interesados de conformidad con el Reglamento general de protección de datos, presentadas por dichos usuarios o sus representantes. Cada responsable del tratamiento designará un punto de contacto específico dedicado a las solicitudes recibidas de los interesados. Si un corresponsable del tratamiento recibe una solicitud de un interesado que no está dentro de su competencia, la remitirá sin demora al corresponsable competente. Si así se les solicita, los corresponsables del tratamiento 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 quince días desde la recepción de la solicitud de ayuda.

([1]) En particular, las especificaciones de interoperabilidad para las cadenas de transmisión transfronterizas entre aplicaciones autorizadas, de 16 de junio de 2020, disponibles en: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0

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 federativa.

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 federativa;

b) todo incidente de seguridad relacionado con la operación de tratamiento en la pasarela federativa;

c) 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;

d) todo incumplimiento de las salvaguardas técnicas u organizativas de la operación de tratamiento en la pasarela federativa.

3) Los corresponsables del tratamiento comunicarán toda violación de la seguridad de los datos personales en relación con la operación de tratamiento en la pasarela federativa 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 (UE) 2016/679 o a raíz de una notificación de la Comisión.

SECCIÓN 3

Evaluación de impacto relativa a la protección de datos

Si un responsable del tratamiento, para cumplir las obligaciones que le imponen los artículos 35 y 36 del Reglamento general de protección de datos, necesita información de otro responsable del tratamiento, enviará una solicitud específica al buzón funcional al que se refiere la sección 1, subsección 1, punto 3. Este último responsable hará lo posible por facilitar esa información.

ANEXO III

RESPONSABILIDADES DE LA COMISIÓN COMO ENCARGADA DEL TRATAMIENTO EN LA PASARELA FEDERATIVA PARA EL TRATAMIENTO TRANSFRONTERIZO DE DATOS ENTRE LAS APLICACIONES MÓVILES NACIONALES DE RASTREO DE CONTACTOS Y ADVERTENCIA

La Comisión:

1) Deberá crear y garantizar una infraestructura de comunicación segura y fiable que interconecte las aplicaciones móviles nacionales de rastreo de contactos y advertencia de los Estados miembros que participen en la pasarela federativa. Para cumplir sus obligaciones como encargada del tratamiento de la pasarela federativa, la Comisión podrá recurrir a terceros como subencargados del tratamiento; deberá informar a los corresponsables del tratamiento de todo cambio previsto que implique la adición o sustitución de otros subencargados, dando así a los responsables del tratamiento la posibilidad de oponerse conjuntamente a tales cambios conforme a la sección 1, subsección 1, punto 4, del anexo II. Asimismo, deberá velar por que se apliquen a estos subencargados del tratamiento las mismas obligaciones de protección de datos que contiene la presente Decisión.

2) Deberá 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.

3) El tratamiento por 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 7 *bis*, apartado 3, de la Decisión de Ejecución, 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 federativa al recibirlos de los servidores finales nacionales;

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

e) la eliminación de los datos cuando todos los servidores finales participantes los hayan descargado, o catorce días después de su recepción si esta fecha es anterior;

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.

El encargado del tratamiento deberá tomar las medidas necesarias para preservar la integridad de los datos tratados.

4) Deberá tomar todas las medidas de seguridad organizativa, física y lógica más avanzadas que sean necesarias para el mantenimiento de la pasarela federativa. Para ello deberá:

a) designar una entidad responsable de la gestión de la seguridad en la pasarela federativa, comunicar a los responsables 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 federativa;

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

5) Deberá 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 federativa. 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. permitir, también a petición de los responsables del tratamiento, la realización de auditorías independientes, en particular inspecciones, y de verificaciones de las medidas de seguridad, en condiciones que respeten lo dispuesto en el Protocolo n.º 7 del TFUE, sobre los privilegios y las inmunidades de la Unión Europea ([2]), y contribuir a ellas;

([2]) Protocolo n.o 7 del TFUE, sobre los privilegios y las inmunidades de la Unión Europea (DO C 326 de 26.10.2012, p. 266).

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 escalamiento, informar sin demora a los responsables del tratamiento y al Supervisor Europeo de Protección de Datos de cualquier violación de la seguridad de los datos personales y definir un procedimiento disciplinario para las violaciones de la seguridad.

6) Deberá adoptar las medidas de seguridad física o lógica más avanzadas para las instalaciones que alojen el equipo de la pasarela federativa y para los controles de los datos lógicos y el acceso de seguridad. Para ello 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 federativa;

f) velar por que las personas que accedan a la pasarela federativa estén identificadas y autenticadas;

g) verificar los derechos de autorización relacionados con el acceso a la pasarela federativa 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 federativa;

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

j) aplicar, cuando sea necesario, medidas para bloquear el acceso no autorizado a la pasarela federativa desde el dominio de las autoridades nacionales (es decir, bloquear una ubicación o una dirección IP).

7) Deberá tomar 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) Deberá mantener un plan de gestión de riesgos relacionado con su ámbito de responsabilidad.

9) Deberá monitorizar, en tiempo real, el funcionamiento de todos los componentes de servicio de sus servicios de la pasarela federativa, elaborar estadísticas regulares y llevar registros.

10) Deberá prestar apoyo con respecto a todos los servicios de la pasarela federativa 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 federativa y sus respectivos servicios de asistencia, los responsables de proyectos y las personas designadas de la Comisión.

11) Deberá ayudar en la medida de lo posible a los responsables del tratamiento con medidas técnicas y organizativas apropiadas, 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) Deberá ayudar a los responsables del tratamiento proporcionándoles información sobre la pasarela federativa, a fin de dar cumplimiento a las obligaciones derivadas de los artículos 32, 35 y 36 del Reglamento general de protección de datos.

13) Deberá garantizar que los datos tratados en la pasarela federativa sean ininteligibles para cualquier persona que no esté autorizada a acceder a ella.

14) Deberá adoptar todas las medidas pertinentes para impedir que los operadores de la pasarela federativa accedan sin autorización a los datos transmitidos.

15) Deberá adoptar medidas para facilitar la interoperabilidad y la comunicación entre los responsables del tratamiento designados de la pasarela federativa.

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