►**B**

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

[notificada con el número C(2019) 7460]

(Texto pertinente a efectos del EEE)

(DO L 270 de 24.10.2019, p. 83)

Modificada por:

		Diario Oficial		
		nº	página	fecha
►**M1**	Decisión de Ejecución (UE) 2020/1023 de la Comisión de 15 de julio de 2020	L 227 I	1	16.7.2020

▼B

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

[notificada con el número C(2019) 7460]

(Texto pertinente a efectos del EEE)

Artículo 1

Objeto

La presente Decisión establece las normas necesarias para el establecimiento, la gestión y el funcionamiento de la red de autoridades nacionales responsables en materia de sanidad electrónica de conformidad con lo dispuesto en el artículo 14, apartado 1, de la Directiva de 2011/24/UE.

Artículo 2

Definiciones

1. A efectos de la presente Decisión, se entenderá por:

a) «red de sanidad electrónica»: la red voluntaria que conecta a las autoridades nacionales encargadas de la sanidad electrónica, designadas por los Estados miembros, y que persigue los objetivos establecidos en el artículo 14 de la Directiva 2011/24/UE;

b) «puntos de contacto nacionales para la sanidad electrónica»: las pasarelas organizativas y técnicas para la prestación de servicios transfronterizos de información de sanidad electrónica bajo la responsabilidad de los Estados miembros;

c) «servicios transfronterizos de información de sanidad electrónica»: los servicios existentes tratados por medio de los puntos de contacto nacionales para la sanidad electrónica y a través de una plataforma central de servicios desarrollada por la Comisión a efectos de la asistencia sanitaria transfronteriza;

d) «infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica»: la infraestructura que posibilita la prestación de servicios transfronterizos de información de sanidad electrónica por medio de los puntos de contacto nacionales para la sanidad electrónica y la plataforma central europea de servicios; esta infraestructura incluye tanto servicios genéricos, según se definen en el artículo 2, apartado 2, letra e), del Reglamento (UE) n.º 283/2014, desarrollados por los Estados miembros, como una plataforma central de servicios, según se define en el artículo 2, apartado 2, letra d), del mismo Reglamento, desarrollada por la Comisión;

e) «otros servicios europeos de sanidad electrónica compartidos»: servicios digitales que pueden desarrollarse en el marco de la red de sanidad electrónica y compartirse entre los Estados miembros;

▼B

f) «modelo de gobernanza»: un conjunto de normas relativas a la designación de los organismos que participan en los procesos decisorios que afectan a la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica o a otros servicios europeos de sanidad electrónica compartidos que se hayan desarrollado en el marco de la red de sanidad electrónica, así como una descripción de dichos procesos;

▼M1

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 ([1]);

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;

([1]) 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).

▼M1

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.

▼B

2. Las definiciones del artículo 4, puntos 1, 2, 7 y 8, del Reglamento (UE) 2016/679 se aplicarán en consecuencia.

Artículo 3

Composición de la red de sanidad electrónica

1. Serán miembros de la red de sanidad electrónica las autoridades de los Estados miembros responsables en materia de sanidad electrónica que designen los Estados miembros que participen en dicha red.

2. Los Estados miembros que deseen participar en la red de sanidad electrónica notificarán por escrito a la Comisión:

a) su decisión de participar en la red de sanidad electrónica;

b) la autoridad nacional responsable en materia de sanidad electrónica que se convertirá en miembro de la red de sanidad electrónica, así como el nombre del representante y el de su suplente.

3. Los Estados miembros notificarán por escrito a la Comisión:

a) su decisión de retirarse de la red de sanidad electrónica;

b) todo cambio en la información a que se refiere el apartado 2, letra b).

4. La Comisión pondrá a disposición del público la lista de miembros participantes en la red de sanidad electrónica.

Artículo 4

Actividades de la red de sanidad electrónica

1. Al perseguir el objetivo contemplado en el artículo 14, apartado 2, letra a), de la Directiva 2011/24/UE, la red de sanidad electrónica podrá, en particular:

a) 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;

b) proporcionar orientación a los Estados miembros, en cooperación con otras autoridades de supervisión competentes, en relación con el intercambio de datos sanitarios entre los Estados miembros y la capacitación de los ciudadanos para acceder a sus datos sanitarios y compartirlos;

▼B

c) proporcionar orientación a los Estados miembros y facilitar el intercambio de buenas prácticas en relación con el desarrollo de diferentes servicios sanitarios digitales, como la telemedicina, la salud móvil o las nuevas tecnologías en el ámbito de los macrodatos y la inteligencia artificial, teniendo en cuenta las acciones en curso a escala de la UE;

d) proporcionar orientación a los Estados miembros en lo que respecta al apoyo a la promoción de la salud, la prevención de enfermedades y la mejora de la prestación de asistencia sanitaria mediante un mejor uso de los datos sanitarios y la mejora de las competencias digitales de los pacientes y los profesionales de la salud;

e) proporcionar orientación a los Estados miembros y facilitar el intercambio voluntario de mejores prácticas sobre las inversiones en infraestructuras digitales;

f) proporcionar orientación a los Estados miembros, en colaboración con otros organismos y partes interesadas pertinentes, sobre los casos de uso necesarios para la interoperabilidad clínica y las herramientas para lograrla;

g) proporcionar orientación a los miembros sobre la seguridad de la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica o para otros servicios europeos de sanidad electrónica compartidos que se desarrollen en el marco de la red de sanidad electrónica, teniendo en cuenta la legislación y los documentos elaborados a nivel de la Unión, en particular en el ámbito de la seguridad, así como recomendaciones en el ámbito de la ciberseguridad, colaborando estrechamente con el Grupo de cooperación en materia de seguridad de las redes y de la información y con las autoridades nacionales, cuando proceda;

▼M1

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.

▼B

2. Al elaborar las directrices en relación con unos métodos eficaces que permitan utilizar los datos médicos en beneficio de la salud pública y la investigación a que se refiere el artículo 14, apartado 2, letra b), inciso ii), de la Directiva 2011/24/UE, la red de sanidad electrónica tendrá en cuenta las directrices adoptadas por el Consejo Europeo de Protección de Datos, al que consultará, en su caso. Estas directrices también podrán abordar la información intercambiada a través de la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica o para otros servicios europeos de sanidad electrónica compartidos.

Artículo 5

Funcionamiento de la red de sanidad electrónica

1. La red de sanidad electrónica aprobará su reglamento interno por mayoría simple de sus miembros.

2. La red de sanidad electrónica adoptará un programa de trabajo plurianual y un instrumento de evaluación de la ejecución de dicho programa.

▼B

3. Para cumplir sus cometidos, la red de sanidad electrónica podrá crear subgrupos permanentes relativos a tareas específicas, en particular en relación con la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica o para otros servicios europeos de sanidad electrónica compartidos que se desarrollen en el marco de la red de sanidad electrónica.

4. La red de sanidad electrónica también podrá crear subgrupos temporales, en particular con expertos, para examinar cuestiones específicas sobre la base de un mandato definido por la propia red. Dichos subgrupos se disolverán tan pronto como hayan cumplido su mandato.

5. Cuando los miembros de la red de sanidad electrónica decidan mejorar su cooperación en algunos ámbitos incluidos en los cometidos de la red, deben acordar las normas de dicha cooperación y comprometerse a cumplirlas.

6. Para alcanzar sus objetivos, la red de sanidad electrónica colaborará estrechamente con las acciones conjuntas que apoyen sus actividades, cuando tales acciones conjuntas existan, con las partes interesadas o con otros organismos o mecanismos de apoyo interesados, y tendrá en cuenta los resultados obtenidos en el marco de dichas actividades.

7. La red de sanidad electrónica elaborará, junto con la Comisión, los modelos de gobernanza de la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica y participará en dicha gobernanza del siguiente modo:

i) acordando las prioridades de la infraestructura de servicios digitales de sanidad electrónica y supervisando su funcionamiento,

ii) elaborando directrices y sus requisitos de funcionamiento, incluida la selección de las normas utilizadas a efectos de la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica,

iii) decidiendo si debe permitirse a los miembros de la red de sanidad electrónica iniciar y continuar el intercambio de datos sanitarios electrónicos a través de la infraestructura de servicios digitales de sanidad electrónica para los servicios de información transfronteriza de sanidad electrónica por medio de sus puntos de contacto nacionales para la sanidad en línea, sobre la base de su conformidad con los requisitos establecidos por la red de sanidad electrónica, según lo evaluado en las pruebas que proporcione la Comisión y las auditorías que lleve a cabo,

iv) aprobando el plan de trabajo anual destinado a la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica.

8. La red de sanidad electrónica podrá elaborar, junto con la Comisión, modelos de gobernanza de otros servicios europeos de sanidad electrónica compartidos que se hayan desarrollado en el marco de la red de sanidad electrónica, y participar en su gobernanza. La red también podrá fijar las prioridades, junto con la Comisión, y elaborar directrices para el funcionamiento de dichos servicios europeos de sanidad electrónica compartidos.

▼B

9. El reglamento interno podrá prever que los países, que no sean Estados miembros, que apliquen la Directiva 2011/24/UE puedan participar en las reuniones de la red de sanidad electrónica en calidad de observadores.

10. Tanto los miembros de la red de sanidad electrónica y sus representantes, como los expertos y observadores invitados guardarán el secreto profesional a que les obliga el artículo 339 del Tratado y respetarán las normas de seguridad de la Comisión relativas a la protección de la información clasificada de la UE, que figuran en la Decisión (UE, Euratom) 2015/444 de la Comisión ([1]). Si no respetan esas obligaciones, el presidente de la red de sanidad electrónica podrá adoptar todas las medidas apropiadas previstas en el reglamento interno.

Artículo 6

Relación entre la red de sanidad electrónica y la Comisión

1. La Comisión:

a) asistirá y copresidirá las reuniones de la red de sanidad electrónica junto con el representante de los miembros;

b) cooperará con la red de sanidad electrónica y le prestará apoyo en relación con sus actividades;

c) se hará cargo de la secretaría de la red de sanidad electrónica;

d) desarrollará, implementará y mantendrá las medidas técnicas y organizativas apropiadas relativas a los servicios básicos de la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica;

e) prestará apoyo a la red de sanidad electrónica a la hora de decidir sobre la conformidad técnica y organizativa de los puntos de contacto nacionales para la sanidad en línea con los requisitos para el intercambio transfronterizo de datos sanitarios, proporcionando y llevando a cabo las pruebas y auditorías necesarias; los expertos de los Estados miembros podrán ayudar a los auditores de la Comisión;

▼M1

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.

▼B

2. La Comisión podrá asistir a las reuniones de los subgrupos de la red de sanidad electrónica.

3. La Comisión podrá consultar a la red de sanidad electrónica sobre cuestiones relacionadas con la sanidad electrónica a nivel de la Unión y el intercambio de mejores prácticas en materia de sanidad electrónica.

([1]) Decisión (UE, Euratom) 2015/444 de la Comisión, de 13 de marzo de 2015, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 72 de 17.3.2015, p. 53).

▼B

4. La Comisión pondrá a disposición del público información sobre las actividades realizadas por la red de sanidad electrónica.

Artículo 7

▼M1

Protección de datos personales tratados a través de la infraestructura de servicios digitales de sanidad electrónica

▼B

1. Los Estados miembros, representados por las autoridades nacionales pertinentes u otros organismos designados, serán considerados responsables del tratamiento de los datos personales que traten a través de la infraestructura de servicios digitales de sanidad electrónica para los servicios de información transfronteriza de sanidad electrónica, y determinarán de manera clara y transparente las responsabilidades respectivas de los responsables del tratamiento.

2. La Comisión será considerada encargada del tratamiento de los datos personales de pacientes que tenga lugar a través de la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica. En su calidad de encargada del tratamiento, la Comisión gestionará los servicios básicos de la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica y cumplirá las obligaciones que incumben a los encargados del tratamiento establecidas en el ►M1 anexo I ◄ de la presente Decisión. La Comisión no tendrá acceso a los datos personales de pacientes tratados a través de la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica.

3. La Comisión será considerada responsable del tratamiento de los datos personales necesarios a efectos de conceder y gestionar los derechos de acceso a los servicios básicos de la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica. Se trata de los datos de contacto de los usuarios, incluidos nombre y apellidos, dirección de correo electrónico y afiliación.

▼M1

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.

▼M1

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.

▼B

Artículo 8

Gastos

1. La Comisión no remunerará los servicios de quienes participen en las actividades de la red de sanidad electrónica.

▼B

2. La Comisión reembolsará los gastos de estancia y desplazamiento de quienes participen en las actividades de la red de sanidad electrónica con arreglo a sus disposiciones vigentes relativas al reembolso de los gastos efectuados por personas ajenas a la Comisión invitadas a participar en reuniones en calidad de expertos. Dichos gastos se reembolsarán dentro del límite de los créditos disponibles que se hayan asignado en el marco del procedimiento anual de asignación de recursos.

Artículo 9

Derogación

Queda derogada la Decisión de Ejecución 2011/890/UE. Las referencias a la Decisión derogada se entenderán hechas a la presente Decisión.

Artículo 10

Destinatarios

Los destinatarios de la presente Decisión son los Estados miembros.

▼M1

ANEXO I

▼B

RESPONSABILIDADES DE LA COMISIÓN COMO ENCARGADA DEL TRATAMIENTO DE DATOS EN LA INFRAESTRUCTURA DE SERVICIOS DIGITALES DE SANIDAD ELECTRÓNICA PARA LOS SERVICIOS TRANSFRONTERIZOS DE INFORMACIÓN DE SANIDAD ELECTRÓNICA

La Comisión:

1. Creará una infraestructura de comunicación que interconecte las redes de los miembros de la red de sanidad electrónica que participen en la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica, y velará por su seguridad y fiabilidad (en lo sucesivo, «infraestructura de comunicación centralizada y segura»). Para cumplir sus obligaciones, la Comisión podrá recurrir a terceros. La Comisión velará por que se apliquen a estos terceros las mismas obligaciones en materia de protección de datos establecidas en la presente Decisión.

2. Configurará parte de la infraestructura de comunicación centralizada y segura para que los puntos de contacto nacionales para la sanidad electrónica puedan intercambiar información de forma segura, fiable y eficiente.

3. La Comisión tratará los datos personales siguiendo instrucciones documentadas de los responsables del tratamiento.

4. Adoptará todas las medidas organizativas, físicas y lógicas de seguridad necesarias para el mantenimiento de la infraestructura de comunicación centralizada y segura. A tal fin, la Comisión:

   a) designará una entidad responsable de la gestión de la seguridad a nivel de la infraestructura de comunicación centralizada y segura, comunicará a los responsables del tratamiento sus datos de contacto y garantizará su disponibilidad para reaccionar ante amenazas para la seguridad;

   b) asumirá la responsabilidad de la seguridad de la infraestructura de comunicación centralizada y segura;

   c) velará por que todas las personas a las que se conceda acceso a la infraestructura de comunicación centralizada y segura estén sujetas a una obligación contractual, profesional o legal de confidencialidad;

   d) velará por que el personal con acceso a información clasificada cumpla los criterios de habilitación y confidencialidad correspondientes.

5. Adoptará todas las medidas de seguridad necesarias para evitar poner en peligro el correcto funcionamiento del dominio de las otras partes. A tal fin, la Comisión instaurará los procedimientos específicos relativos a la conexión a la infraestructura de comunicación centralizada y segura. Estos incluirán:

   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 aplicada,

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

      iii) detectar violaciones de la seguridad e intrusiones,

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

▼B

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;

c) un procedimiento de control de los cambios para documentar y medir el impacto de un cambio antes de su aplicación y mantener informados a los puntos de contacto nacionales para la sanidad electrónica sobre cualquier modificación que pueda afectar a la comunicación con otras infraestructuras nacionales o a su seguridad;

d) un procedimiento de mantenimiento y reparación para especificar las normas y condiciones que deben cumplirse en caso de que deba procederse al mantenimiento o reparación de equipos;

e) un procedimiento en caso de producirse un incidente de seguridad para definir el régimen de notificación y transmisión de la información, informar sin demora a la administración nacional responsable, así como al Supervisor Europeo de Protección de Datos, de cualquier violación de la seguridad y definir un procedimiento disciplinario en caso de violaciones de la seguridad.

6. Adoptará medidas de seguridad físicas o lógicas para las instalaciones que alojen el equipo de la infraestructura de comunicación centralizada y segura y para los controles de los datos lógicos y el acceso de seguridad. A tal fin, la Comisión:

a) aplicará medidas de seguridad física para establecer perímetros de seguridad específicos y que permitan detectar las violaciones;

b) controlará el acceso a las instalaciones y mantendrá un registro de visitantes a efectos de localización;

c) velará por que las personas externas a las que se haya concedido acceso a las instalaciones sean acompañadas por personal debidamente autorizado de su organización;

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

e) controlará el acceso desde y hacia otras redes interconectadas a la infraestructura de comunicación centralizada y segura;

f) velará por que las personas que accedan a la infraestructura de comunicación centralizada y segura sean identificadas y autenticadas;

g) verificará los derechos de autorización relacionados con el acceso a la infraestructura de comunicación centralizada y segura en caso de que se produzca una violación de la seguridad que afecte a esta infraestructura;

h) mantendrá la integridad de la información transmitida a través de la infraestructura de comunicación centralizada y segura;

i) implementará medidas técnicas y organizativas de seguridad para evitar el acceso no autorizado a datos personales;

j) implementará, cuando sea necesario, medidas para bloquear el acceso no autorizado a la infraestructura de comunicación centralizada y segura desde el dominio de los puntos de contacto nacionales para la sanidad electrónica (por ejemplo, bloqueo de una ubicación/dirección IP).

7. Tomará 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. Mantendrá un plan de gestión de riesgos relacionado con su ámbito de responsabilidad.

▼B

9. Supervisará, en tiempo real, el desempeño de todos los componentes de servicio de los servicios de la infraestructura de comunicación centralizada y segura, elaborará estadísticas regulares y llevará registros.

10. Prestará apoyo a todos los servicios de la infraestructura de comunicación centralizada y segura en inglés, 24/7, por teléfono, correo electrónico o portal web, y aceptará llamadas de usuarios autorizados: coordinadores de la infraestructura de comunicación centralizada y segura y sus respectivos servicios de asistencia, responsables de proyectos y personas designadas de la Comisión.

11. Apoyará a los responsables del tratamiento facilitando información relativa a la infraestructura de comunicación centralizada y segura de la infraestructura de servicios digitales de sanidad electrónica para los servicios transfronterizos de información de sanidad electrónica, con el fin de cumplir las obligaciones establecidas en los artículos 35 y 36 del Reglamento (UE) 2016/679.

12. Velará por que los datos que se transfieran en la infraestructura de comunicación centralizada y segura estén cifrados.

13. Adoptará todas las medidas pertinentes para impedir que los operadores de la infraestructura de comunicación centralizada y segura accedan sin autorización a los datos transferidos.

14. Adoptará medidas para facilitar la interoperabilidad y la comunicación entre las administraciones nacionales competentes designadas de la infraestructura de comunicación centralizada y segura.

▼M1

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

([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

▼M1

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.

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.

▼M1

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:

▼M1

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 ([1]), y contribuir a ellas;

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:

([1]) 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).

▼M1

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.

▼**M1**

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..