RECOMENDACIONES

RECOMENDACIÓN DE LA COMISIÓN

de 6 de febrero de 2012

sobre directrices para la protección de datos en el sistema de alerta precoz y respuesta (SAPR)

[notificada con el número C(2012) 568]

(Texto pertinente a efectos del EEE)

(2012/73/UE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 292,

Previa consulta al Supervisor Europeo de Protección de Datos,

Considerando lo siguiente:

(1) Mediante la Decisión nº 2119/98/CE del Parlamento Europeo y del Consejo, de 24 de septiembre de 1998, por la que se crea una red de vigilancia epidemiológica y de control de las enfermedades transmisibles en la Comunidad [1] se estableció una red de vigilancia epidemiológica y de control de las enfermedades transmisibles en la Comunidad, y un sistema de alerta precoz y respuesta (SAPR) para la prevención y el control de estas enfermedades.

(2) En su Decisión 2000/57/CE, de 22 de diciembre de 1999, relativa al sistema de alerta precoz y respuesta para la vigilancia y control de las enfermedades transmisibles en aplicación de la Decisión nº 2119/98/CE del Parlamento Europeo y del Consejo [2], la Comisión adoptó disposiciones de aplicación del SAPR, para que ella y las autoridades sanitarias competentes de los Estados miembros del Espacio Económico Europeo estén en contacto estructurado y permanente, mediante los medios apropiados, a fin de determinar las medidas que puedan ser necesarias para proteger la salud pública y prevenir y detener la propagación de las enfermedades transmisibles [3].

(3) El derecho a la protección de los datos personales está reconocido en la Carta de los Derechos Fundamentales de la Unión Europea, concretamente en su artículo 8.

(4) Además, el intercambio electrónico de información entre los Estados miembros, y entre estos y la Comisión, debe atenerse a las normas sobre protección de datos personales previstas en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [4], y en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos [5].

(5) La Decisión 2009/547/CE de la Comisión, de 10 de julio de 2009, por la que se modifica la Decisión 2000/57/CE, relativa al sistema de alerta precoz y respuesta para la vigilancia y control de las enfermedades transmisibles en aplicación de la Decisión nº 2119/98/CE del Parlamento Europeo y del Consejo [6] introduce garantías específicas para el intercambio de datos personales entre los Estados miembros en el proceso de identificar a las personas infectadas o que puedan estar en peligro, cuando se produce un hecho relacionado con enfermedades transmisibles de posible repercusión en toda la UE.

(6) El 26 de abril de 2010, el Supervisor Europeo de Protección de Datos (SEPD) emitió un dictamen de control previo [7] en el que pedía se aclarase la responsabilidad de

[1] DO L 268 de 3.10.1998, p. 1.
[2] DO L 21 de 26.1.2000, p. 32.
[3] El SAPR se reserva para la notificación, por las autoridades sanitarias competentes de los Estados miembros, de determinados hechos definidos en el anexo I de la Decisión 2000/57/CE («los hechos») que puedan constituir amenazas para la salud pública.
[4] DO L 281 de 23.11.1995, p. 31.
[5] DO L 8 de 12.1.2001, p. 1.
[6] DO L 181 de 14.7.2009, p. 57.
[7] Dictamen de control previo de 26 de abril de 2010 del SEPD sobre el SAPR, notificado por la Comisión Europea el 18 de febrero de 2009 (asunto C 2009-0137). Está publicado en el sitio web del SEPD: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2010/10-04-26_EWRS_EN.pdf

cada interviniente en el SAPR, para abordar adecuadamente los riesgos que una gran amenaza pandémica plantearía para los derechos fundamentales durante el proceso de trazabilidad de contactos a gran escala.

(7) Teniendo en cuenta las recomendaciones del SEPD en su dictamen, la Comisión ha elaborado unas directrices para la protección de datos en el SAPR, para contribuir a aclarar las respectivas funciones, tareas y obligaciones de cada agente del sistema, y así garantizar el cumplimiento efectivo de las mencionadas normas de protección de datos y el suministro de información clara y mecanismos fácilmente accesibles para que los interesados hagan valer sus derechos.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

1. Los Estados miembros deben alertar a los usuarios del SAPR sobre las directrices que figuran en el anexo de la presente Recomendación.

2. Conviene exhortar a los coordinadores nacionales del SAPR a que soliciten a sus autoridades nacionales de protección de datos orientación y asistencia sobre la mejor manera de aplicar las presentes directrices en el marco de la normativa nacional.

3. Se recomienda a los Estados miembros que informen a la Comisión Europea sobre la aplicación de las directrices recogidas en el anexo, a más tardar dos años después de la adopción de la presente Recomendación. La Comisión compartirá con el SEPD esta información y la tendrá en cuenta para evaluar el nivel de protección de datos en el SAPR, el contenido y el calendario de futuras medidas, como la posible adopción de un instrumento jurídico.

4. Los destinatarios de la presente Recomendación serán los Estados miembros.

Hecho en Bruselas, el 6 de febrero de 2012.

Por la Comisión

John DALLI

Miembro de la Comisión

ANEXO

DIRECTRICES PARA LA PROTECCIÓN DE DATOS EN EL SISTEMA DE ALERTA PRECOZ Y RESPUESTA (SAPR)

1. INTRODUCCIÓN

El SAPR es una aplicación web diseñada por la Comisión Europea, en cooperación con los Estados miembros, para que ella y las autoridades sanitarias competentes de los Estados miembros del EEE estén en contacto estructurado y permanente a fin de determinar las medidas necesarias para proteger la salud pública. El Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC), Agencia de la UE, también está conectado al SAPR desde 2005 [1].

La cooperación entre las autoridades sanitarias nacionales es vital para mejorar la capacidad de los Estados miembros de prevenir la propagación de enfermedades transmisibles en la UE, así como de responder coordinadamente y a tiempo a hechos causados por enfermedades transmisibles que sean, o puedan llegar a ser, amenazas para la salud pública.

Anteriores brotes de neumonía coronavírica, de gripe A (H1N1) pandémica y otras enfermedades transmisibles han demostrado con claridad lo rápidamente que pueden propagarse enfermedades antes desconocidas, de elevada morbimortalidad, que no respetan fronteras, favorecidas por la rapidez de los desplazamientos y el comercio mundial. La detección temprana y la comunicación y coordinación eficaces a escala europea e internacional son esenciales para controlar tales contingencias y evitar su evolución devastadora.

El SAPR se diseñó como un mecanismo centralizado para que los Estados miembros envíen alertas, compartan información y coordinen su respuesta, de modo oportuno y seguro, en relación con hechos que puedan constituir una amenaza sanitaria para la UE.

2. ÁMBITO DE APLICACIÓN Y OBJETIVOS DE LAS DIRECTRICES

La gestión y el uso del SAPR pueden requerir el intercambio de datos personales en algunos casos previstos por los instrumentos jurídicos pertinentes (véase el punto 4 relativo al fundamento jurídico del intercambio de datos personales en el SAPR).

El intercambio de información personal entre las autoridades sanitarias competentes de los Estados miembros debe cumplir las normas de protección de datos personales establecidas en las legislaciones nacionales por las que se transpone la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Sin embargo, como los usuarios del SAPR no son expertos en protección de datos y pueden no ser siempre conscientes de los requisitos que la ley impone al respecto, conviene ofrecerles unas directrices que expliquen el funcionamiento del SAPR en cuanto a la protección de datos, de forma sencilla y fácilmente comprensible. También se persigue con las directrices aumentar la sensibilización, promover las mejores prácticas y difundir entre los usuarios de los Estados miembros un planteamiento coherente y uniforme de la protección de datos.

No obstante, hay que recalcar que las presentes directrices no pretenden examinar exhaustivamente todo lo relativo a la protección de los datos en el marco del SAPR. Puede obtenerse más orientación y asistencia de las autoridades responsables de la protección de datos («la autoridad de control») en los Estados miembros. En particular, se recomienda encarecidamente a los usuarios del SAPR consultar con sus autoridades de control la mejor manera de aplicar las presentes directrices en su país, de modo que se cumplan íntegramente los requisitos nacionales específicos de protección de datos. La lista de las autoridades de control con sus señas puede consultarse en la siguiente dirección:

http://ec.europa.eu/justice/policies/privacy/nationalcomm/index_en.htm

Por último, hay que subrayar que las presentes directrices no son una interpretación auténtica de la legislación de la UE sobre protección de datos, pues en el sistema institucional de la Unión la interpretación de la legislación de la UE recae exclusivamente en el Tribunal de Justicia.

3. DERECHO APLICABLE Y SUPERVISIÓN

La determinación de la legislación aplicable depende de quién es el usuario del SAPR. Concretamente, el tratamiento de los datos personales por la Comisión y el ECDC, en el marco de la gestión y el funcionamiento del sistema (como se muestra en los siguientes puntos) se rige por el Reglamento (CE) nº 45/2001.

[1] El ECDC también apoya y ayuda a la Comisión en la gestión de la aplicación del SAPR, tarea que le asignó el Reglamento (CE) nº 851/2004 del Parlamento Europeo y del Consejo, de 21 de abril de 2004, por el que se creó y, en particular, su artículo 8 (DO L 142 de 30.4.2004, p. 1).

En el caso del tratamiento de los datos personales por las autoridades nacionales competentes del SAPR, es aplicable la correspondiente legislación nacional por la que se transpone la Directiva 95/46/CE. Debe tenerse en cuenta que esta Directiva deja cierto margen de maniobra a los Estados miembros para transponer sus disposiciones al Derecho nacional. En particular, la Directiva permite que los Estados miembros introduzcan exenciones o excepciones a algunas de sus disposiciones en casos específicos. Al mismo tiempo, la legislación nacional de protección de datos que ha de respetar el usuario del SAPR puede establecer requisitos más estrictos, o propios del país, no previstos en la legislación de otros Estados miembros.

Habida cuenta de estas peculiaridades, se aconseja a los usuarios del SAPR consultar las presentes directrices con sus respectivas autoridades de control, de modo que se cumplan íntegramente los requisitos nacionales aplicables. Por ejemplo, la información concreta que debe proporcionarse a los interesados al recoger los datos puede diferir significativamente de un Estado miembro a otro, así como las normas para el tratamiento de categorías especiales de datos personales (por ejemplo, sobre la salud).

Una de las principales características del marco jurídico de la UE sobre protección de datos, consistente en el Reglamento (CE) nº 45/2001 y la Directiva 95/46/CE, es su supervisión por autoridades públicas e independientes de protección de datos. El Supervisor Europeo de Protección de Datos (SEPD) [1] controla el tratamiento de datos personales por las instituciones y organismos de la UE, mientras que las autoridades de control de cada Estado miembro se ocupan del tratamiento de los datos por personas físicas o jurídicas, autoridades públicas nacionales, agencias y demás organismos nacionales. Todos los Estados miembros han designado autoridades de supervisión para ocuparse de las reclamaciones presentadas por los ciudadanos en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Para mayor información sobre cómo gestionar las quejas o las solicitudes individuales, los usuarios del SAPR pueden consultar el punto 9, sobre el acceso a los datos personales y otros derechos de los interesados.

4. FUNDAMENTO JURÍDICO DEL INTERCAMBIO DE DATOS PERSONALES EN EL SAPR

Mediante la Decisión 2119/98/CE del Parlamento Europeo y del Consejo se estableció una red a escala de la Unión («la red») para fomentar, con ayuda de la Comisión, la cooperación y coordinación entre los Estados miembros para mejorar la prevención y el control de las enfermedades transmisibles en la UE [2]. Uno de los pilares de la red es el SAPR, que permite intercambiar información, consultarse y coordinarse a nivel europeo cuando se produce un hecho relacionado con enfermedades transmisibles de posible repercusión para la salud pública en toda la UE.

Conviene recalcar que no toda la información intercambiada en el SAPR es de carácter personal. En realidad, generalmente en este marco no se intercambian datos personales, sanitarios ni de otro tipo, de personas físicas identificadas o identificables.

¿Qué son «datos personales»?

A efectos de la Directiva 95/46/CE y del Reglamento (CE) nº 45/2001, se entiende por «datos personales» toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social [3].

Las autoridades sanitarias competentes de los Estados miembros del EEE comunican a la red a través del SAPR, sobre todo informaciones relativas al brote o reaparición de casos de enfermedades transmisibles, junto con la información relativa a las medidas de control aplicadas, o información sobre fenómenos epidemiológicos infrecuentes o nuevas enfermedades transmisibles de origen desconocido [4] cuya contención pueda exigir la actuación oportuna y coordinada de los Estados miembros [5]. Los Estados miembros, basándose en la información disponible a través de la red, se consultarán entre sí y en contacto con la Comisión, con vistas a coordinar sus esfuerzos de prevención y control de las enfermedades transmisibles, en particular en lo relativo a las medidas nacionales que hayan adoptado o vayan a adoptar [6].

Sin embargo, en algunos casos, la información intercambiada sí que es relativa a personas concretas, por lo que puede considerarse «datos personales».

En primer lugar, hay que decir que el tratamiento de una cantidad limitada de datos personales de los usuarios autorizados del SAPR es inherente a la gestión y operación del sistema. De hecho, tratar los datos de contacto de los usuarios (nombre, organización, correo electrónico, teléfono, etc.) es esencial para establecer y operar el sistema. Los Estados miembros recaban estos datos personales, que vuelven a ser tratados bajo responsabilidad de la Comisión, únicamente a efectos de una cooperación eficaz para la gestión del SAPR y la red subyacente.

[1] http://www.edps.europa.eu/EDPSWEB/edps/EDPS
[2] Las categorías de enfermedades transmisibles incluidas en la red se limitan a las que figuran en el anexo de la Decisión nº 2119/98/CE.
[3] Artículo 2, letra a), de la Directiva 95/46/CE y artículo 2, letra a), del Reglamento (CE) nº 45/2001.
[4] Artículo 4 de la Decisión nº 2119/98/CE.
[5] Anexo I de la Decisión 2000/57/CE, sobre la definición de «hechos» que deben comunicarse mediante el SAPR.
[6] Artículo 6 de la Decisión nº 2119/98/CE.

Lo que es más importante, cuando se produce un hecho relacionado con enfermedades transmisibles de posible repercusión en toda la UE puede obligarse a los Estados miembros afectados a establecer, en régimen de colaboración, medidas específicas de control, las denominadas medidas «de trazabilidad», para identificar a las personas infectadas o que puedan estar en peligro y para impedir la propagación de enfermedades transmisibles graves. Esta colaboración puede consistir en el intercambio a través del SAPR, entre los Estados miembros directamente afectados por las medidas de trazabilidad de los contactos, de datos personales, incluso datos sanitarios confidenciales, de casos humanos confirmados o presuntos ([1]).

¿Qué es «tratamiento de datos personales»?

A efectos de la Directiva 95/46/CE y del Reglamento (CE) nº 45/2001, se entiende por tratamiento de datos personales «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción» ([2]).

En los casos mencionados, el tratamiento de datos personales en el SAPR debe estar justificado por motivos jurídicos específicos. A este respecto, el artículo 7 de la Directiva 95/46/CE y las disposiciones correspondientes del artículo 5 del Reglamento (CE) nº 45/2001 establecen los criterios que legitiman el tratamiento de los datos.

El tratamiento de los datos de contacto de los usuarios del SAPR se basa en:

— el artículo 5, letra b), del Reglamento (CE) nº 45/2001: «solo podrá efectuarse si es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento» ([3]). El tratamiento es necesario para la gestión y operación del SAPR por la Comisión, con el apoyo del ECDC;

— y en el artículo 5, letra d), del Reglamento (CE) nº 45/2001: «el interesado ha dado su consentimiento de forma inequívoca». Los datos de contacto de los usuarios se obtienen de los propios interesados, después de haberles comunicado las condiciones de su consentimiento con conocimiento de causa a que sus datos personales sean tratados en el SAPR (véase el punto 8 sobre la comunicación de información a los interesados).

Los criterios establecidos en el artículo 7, letras c), d) y e), de la Directiva 95/46/CE son los más pertinentes para intercambiar datos de trazabilidad de contactos (señas de la persona infectada, transporte y demás datos relativos al itinerario de viaje de la persona, lugares de estancia, personas visitadas y personas que han podido verse expuestas al contagio) de personas del SAPR ([4]):

— artículo 7, letra c), de la Directiva 95/46/CE: «es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento». La Decisión 2119/98/CE exige la creación de un SAPR para la prevención y el control de las enfermedades transmisibles en la UE. La Decisión impone a los Estados miembros la obligación de notificar mediante el SAPR ciertos hechos provocados por enfermedades contagiosas que constituyan o puedan llegar a constituir amenazas para la salud pública ([5]). La obligación de notificación cubre también las medidas tomadas por las autoridades competentes de los Estados miembros para prevenir y detener la propagación de estas enfermedades, incluidas las medidas de trazabilidad de los contactos destinadas a localizar a las personas infectadas o que puedan estarlo ([6]);

— artículo 7, letra d), de la Directiva 95/46/CE: «es necesario para proteger el interés vital del interesado». En principio, es necesario que los Estados miembros afectados intercambien los datos personales de las personas infectadas o que puedan estarlo, al objeto de ofrecerles la asistencia o el tratamiento adecuado, así como para poder localizarlos e identificarlos con fines de aislamiento y cuarentena, al objeto de proteger la salud de las personas afectadas y, en última instancia, la del conjunto de los ciudadanos de la Unión, y

— artículo 7, letra e), de la Directiva 95/46/CE: «es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos». El SAPR es una herramienta concebida para ayudar a los Estados miembros a coordinar sus esfuerzos de prevención y control de enfermedades transmisibles graves en la UE, es decir, para realizar una tarea de interés público encomendada a los Estados miembros: proteger la salud pública.

([1]) La inclusión de la «trazabilidad de los contactos» entre los fines legítimos para tratar datos personales en el SAPR es el resultado de las modificaciones introducidas en la Decisión 2000/57/CE de la Comisión mediante la Decisión 2009/547/CE.
([2]) Artículo 2, letra b), de la Directiva 95/46/CE y artículo 2, letra b), del Reglamento (CE) nº 45/2001.
([3]) Para la definición de «responsable del tratamiento», véase el punto 5.
([4]) En anexo a la Decisión 2009/547/CE figura una lista indicativa de datos personales que puedan intercambiarse a efectos de la trazabilidad de los contactos.
([5]) Artículo 1 y anexo I de la Decisión 2000/57/CE, en cuanto a la definición de «hechos» que deben comunicarse mediante el SAPR.
([6]) Artículo 2 *bis* de la Decisión 2000/57/CE, introducido por la Decisión 2009/547/CE.

Esas mismas razones de interés público pueden justificar que los Estados miembros traten en el SAPR datos sanitarios sensibles, como información sobre hechos que supongan una amenaza para la salud y datos sobre la salud de las personas infectadas o que puedan estar expuestas al contagio. Aunque el tratamiento de los datos relativos a la salud está en principio prohibido por el artículo 8, apartado 1, de la Directiva 95/46/CE, el tratamiento de esta categoría especial de datos en el SAPR está cubierto por la exención establecida en el artículo 8, apartado 3, de dicha Directiva, que establece que la prohibición no se aplicará cuando el tratamiento de datos «resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto».

La legislación nacional, o una decisión de las autoridades de control en los Estados miembros, pueden permitir otras exenciones de la prohibición de tratar datos sanitarios personales, por motivos fundamentados de interés público y siempre que se den las garantías adecuadas ([1]).

5. ¿QUIÉN ES QUIÉN EN EL SAPR? LA CUESTIÓN DE LA RESPONSABILIDAD COMPARTIDA

El SAPR se diseñó con una técnica para interconectar, mediante diversos canales de comunicación estructurada, múltiples usuarios: las personas de contacto designadas por las autoridades sanitarias competentes de los Estados miembros del EEE (los «puntos de contacto del SAPR»), la Comisión, el ECDC y, en cierta medida, también la OMS.

Cada uno de estos intervinientes del SAPR es un usuario independiente del sistema, aunque el acceso a la información intercambiada en el sistema haya sido modulado mediante la creación de diversos perfiles de usuario y de canales de comunicación «selectivos», que conllevan salvaguardias apropiadas para asegurar el cumplimiento de las normas de protección de datos.

Concretamente, el sistema tiene dos canales principales de comunicación. El primero, el de «mensajes generales», para que las autoridades sanitarias competentes de un Estado miembro comuniquen a todos los puntos de contacto del SAPR, a la Comisión, al ECDC y a la OMS información sobre hechos relacionados con enfermedades transmisibles de posible repercusión para la salud pública en toda la UE, de notificación obligatoria a tenor de la Decisión 2119/98/CE ([2]).

Normalmente, por este canal de mensajes generales no se comunica información sanitaria ni otros datos de personas físicas identificadas o identificables. El sistema lleva salvaguardias específicas para evitar que en este canal se traten datos de modo ilícito (véase el punto 7).

Sin embargo, la aparición de hechos causados por enfermedades transmisibles de posible repercusión para la salud pública en toda la UE puede obligar a los Estados miembros afectados a establecer, en régimen de colaboración, medidas específicas de trazabilidad para identificar a las personas infectadas o que puedan verse expuestas al contagio y para impedir la propagación de enfermedades transmisibles graves.

Para garantizar el cumplimiento de las normas de protección de datos, se han introducido salvaguardias apropiadas para limitar el intercambio de datos de trazabilidad de los contactos y datos sanitarios de personas físicas únicamente a los Estados miembros afectados directamente por un determinado procedimiento de trazabilidad de contactos, e impedir a los demás Estados miembros de la red, a la Comisión y al ECDC el acceso a estos datos ([3]).

Con este fin se estableció el segundo canal, el de «mensajes selectivos», que dota al SAPR de un canal de comunicación exclusivo entre los Estados miembros afectados por una determinada medida de trazabilidad de contactos.

Al intercambiar datos personales a través del canal de mensajes selectivos, las autoridades competentes adoptan el papel de «responsable del tratamiento» de dichos datos, asumiendo así la responsabilidad de la legitimidad de sus actividades de tratamiento y de velar por el cumplimiento de las obligaciones de protección de datos establecidas en la legislación nacional por la que se transpone la Directiva 95/46/CE.

([1]) Según lo previsto en el artículo 8, apartado 4, de la Directiva 95/46/CE.
([2]) Véanse, en particular, sus artículos 4, 5 y 6.
([3]) Artículo 2 *bis* de la Decisión 2000/57/CE, introducido por la Decisión 2009/547/CE.

¿Quién es el «responsable del tratamiento»?

A efectos de la Directiva 95/46/CE, se entiende por responsable del tratamiento «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales» ([1]).

En principio, los usuarios de la Comisión y del ECDC no tienen acceso a los datos personales intercambiados a través del canal de mensajes selectivos ([2]). Sin embargo, por razones técnicas, el almacenamiento central de datos en el SAPR es responsabilidad última de la Comisión, como administradora del sistema y coordinadora. Como tal, la Comisión es también responsable del registro, almacenamiento y tratamiento de los datos personales de los usuarios autorizados del SAPR, necesarios para el funcionamiento del sistema.

Por todo lo dicho, el SAPR es un claro ejemplo de responsabilidad compartida a diferentes niveles entre la Comisión y los Estados miembros para garantizar la protección de los datos personales. En 2005, por otra parte, la Comisión y los Estados miembros, como corresponsables del tratamiento de los datos, decidieron delegar la gestión diaria de la aplicación informática del SAPR al ECDC. Además de esta delegación, la Agencia ha asumido la responsabilidad de garantizar, como «encargada del tratamiento», la confidencialidad y la seguridad de las operaciones de tratamiento efectuadas dentro del sistema, de conformidad con las obligaciones establecidas en los artículos 21 y 22 del Reglamento (CE) nº 45/2001.

¿Quién es el «encargado del tratamiento» y cuáles son sus obligaciones?

A efectos del Reglamento (CE) nº 45/2001, se entiende por encargado del tratamiento «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento» ([3]).

El Reglamento prevé que, cuando una operación de tratamiento se realice por cuenta del responsable, este elija un encargado del tratamiento que reúna garantías suficientes en relación con las medidas técnicas y organizativas necesarias para la seguridad de los datos. El responsable del tratamiento es el responsable último del cumplimiento de dichas medidas. No obstante, las obligaciones de confidencialidad y seguridad del tratamiento contempladas en los artículos 21 y 22 del Reglamento también incumben al encargado ([4]).

6. PRINCIPIOS APLICABLES DE PROTECCIÓN DE DATOS

El tratamiento de datos personales en el SAPR debe cumplir los principios de protección de datos establecidos en el Reglamento (CE) nº 45/2001 y en la Directiva 95/46/CE.

Como responsables del tratamiento, la Comisión y las autoridades competentes de los Estados miembros tienen que velar por el cumplimiento de estos principios cada vez que traten datos personales en el SAPR. Se presentan a continuación los principios fundamentales de la protección de datos, sin perjuicio de otros requisitos aplicables de protección de datos establecidos en los instrumentos jurídicos pertinentes, sobre los que se dan elementos orientativos en otros puntos de las presentes directrices. Concretamente, los usuarios del SAPR deben leer atentamente el punto 8, sobre comunicación de información a los interesados, y el punto 9, sobre el acceso a los datos personales y otros derechos de los interesados.

6.1. *Principios de licitud del tratamiento de datos y limitación de la finalidad*

Los responsables del tratamiento deben velar por que los datos personales sean tratados de manera leal y lícita. Este principio implica, en primer lugar, que la recogida y el tratamiento ulterior de datos personales deben responder a motivos legítimos previstos por la ley ([5]). En segundo lugar, los datos personales solo podrán ser recogidos con fines determinados, explícitos y legítimos, y no podrán ser tratados posteriormente de manera incompatible con dichos fines ([6]).

([1]) Artículo 2, letra d), de la Directiva 95/46/CE.

([2]) En circunstancias excepcionales, la Comisión puede participar en el intercambio de datos personales por el canal de mensajes selectivos del SAPR cuando sea absolutamente necesario coordinar o permitir la rápida y eficaz aplicación de medidas de salud pública con arreglo a la Decisión nº 2119/98/CE y sus disposiciones de aplicación. En esos casos, la Comisión velará por la licitud del tratamiento y por que se lleve a cabo de conformidad con lo dispuesto en el Reglamento (CE) nº 45/2001.

([3]) Artículo 2, letra e), del Reglamento (CE) nº 45/2001.

([4]) Estos principios están recogidos en el artículo 23, apartado 1, del Reglamento (CE) nº 45/2001 sobre el tratamiento de datos personales por cuenta de los responsables del tratamiento.

([5]) El principio de la licitud del tratamiento se deriva de las disposiciones conjuntas del artículo 6, apartado 1, letra a), del artículo 7 y del artículo 8 de la Directiva 95/46/CE. Véanse también las correspondientes disposiciones del Reglamento (CE) nº 45/2001.

([6]) El principio de la limitación de los fines está enunciado en el artículo 6, apartado 1, letra b), de la Directiva 95/46/CE y en la correspondiente disposición del artículo 4, apartado 1, letra b), del Reglamento (CE) nº 45/2001.

6.2. *Principio de calidad de los datos*

Los responsables del tratamiento deben velar por que los datos personales sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben. Además, los datos deben ser exactos y actualizados ([1]).

6.3. *Principio de conservación de los datos*

Los responsables del tratamiento deben velar por que los datos personales sean conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente ([2]).

6.4. *Principios de confidencialidad y seguridad del tratamiento de los datos*

Los responsables del tratamiento deben velar por que las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo traten datos personales a los que tengan acceso cuando se lo encargue el responsable del tratamiento ([3]). Además, los responsables del tratamiento deben aplicar las medidas técnicas y organizativas adecuadas para proteger los datos personales contra la destrucción, pérdida, alteración, difusión o acceso accidentales, no autorizados o ilícitos, y contra cualquier otro tratamiento ilícito de datos personales ([4]).

Con vistas a una aplicación correcta y efectiva de los principios mencionados al utilizar la red, se recomienda a los usuarios del SAPR, en particular, que:

Para estar seguros de que la operación de tratamiento tiene fundamento jurídico, que los datos se recogen para fines legítimos y explícitos y que después no son tratados de manera incompatible con dichos fines, cada vez que recaben o traten datos personales a través del SAPR, los usuarios:

— deben evaluar caso por caso si está justificado aplicar medidas coordinadas de trazabilidad de los contactos, lo que conlleva la activación del canal de mensajes selectivos del SAPR para intercambiar datos personales y de trazabilidad de contactos, habida cuenta de la naturaleza de la enfermedad y del fundamento científico de que la trazabilidad permita prevenir o reducir la propagación de la enfermedad, según la evaluación del riesgo realizada por las autoridades sanitarias de los Estados miembros y por organismos científicos como el ECDC y la OMS;

— no deben utilizar el canal de mensajes generales para intercambiar información de trazabilidad de los contactos ni otros datos personales. Concretamente, deben velar por que tales datos no figuren en el cuerpo de los mensajes generales que envíen, en los anexos ni de cualquier otra forma. La utilización del canal de mensajes generales para la trazabilidad de los contactos sería ilegítima y desproporcionada, pues habría datos personales que quedarían desvelados a destinatarios (como la Comisión y el ECDC) no directamente afectados por un determinado procedimiento de trazabilidad de los contactos y que no necesitan tener acceso a dichos datos;

— al utilizar la función de mensajes selectivos, deben plantearse la «necesidad de saber», es decir, los destinatarios de mensajes selectivos con datos de carácter personal serán solo las autoridades competentes de los Estados miembros que tengan que cooperar en un determinado procedimiento de trazabilidad de los contactos.

Los usuarios del SAPR deben prestar especial atención al intercambiar por mensajería selectiva datos sensibles sobre la salud de una persona identificada o identificable; por ejemplo, personas infectadas o expuestas al contagio cuyos datos de contacto o demás informaciones personales se vayan a revelar a través del SAPR, de manera que la persona en cuestión pueda ser identificada directa o indirectamente. En este caso, siguen siendo aplicables todas las recomendaciones mencionadas y, además, los usuarios del SAPR deben recordar que la Directiva 95/46/CE solo autoriza el intercambio de datos sensibles en circunstancias muy limitadas. Concretamente ([5]):

— cuando el interesado haya dado su consentimiento explícito a dicho tratamiento [artículo 8, apartado 2, letra a), de la Directiva 95/46/CE]. No obstante, la necesidad de intervenir a tiempo en situaciones de emergencia sanitaria puede impedir ofrecer a los interesados toda la información necesaria para que puedan dar su consentimiento con conocimiento de causa (véase el punto 8, sobre la comunicación de información a los interesados). También puede ocurrir que en el momento de recabar los datos se desconozca que podrían llegar a hacerse públicos a través del SAPR;

([1]) Artículo 6, apartado 1, letras c) y d), de la Directiva 95/46/CE y artículo 4, apartado 1, letras c) y d), del Reglamento (CE) nº 45/2001.
([2]) Artículo 6, apartado 1, letra e), de la Directiva 95/46/CE y artículo 4, apartado 1, letra e), del Reglamento (CE) nº 45/2001.
([3]) El principio de confidencialidad está establecido en el artículo 16 de la Directiva 95/46/CE y en la disposición correspondiente del artículo 21 del Reglamento (CE) nº 45/2001.
([4]) El principio de seguridad está establecido en el artículo 17 de la Directiva 95/46/CE y en la disposición correspondiente del artículo 22 del Reglamento (CE) nº 45/2001.
([5]) Para conocer todas las exenciones a la prohibición del tratamiento de determinadas categorías especiales de datos, como los sanitarios, véase el artículo 8, apartados 2, 3, 4 y 5, de la Directiva 95/46/CE.

— a falta de consentimiento de los interesados, el tratamiento de datos sanitarios puede considerarse legítimo si es necesario «para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios», siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional, o por otra persona sujeta asimismo a una obligación equivalente de secreto (artículo 8, apartado 3, de la Directiva 95/46/CE). Dicho de otro modo, cada vez que envíen por mensajería selectiva datos sanitarios sensibles a destinatarios de otros Estados miembros, los usuarios del SAPR deben evaluar si su difusión es estrictamente necesaria para que las autoridades competentes de los Estados miembros afectados tomen las medidas específicas requeridas para alguno de los fines mencionados. Asimismo se recuerda a los usuarios del SAPR que pueden existir otras razones para el tratamiento de datos sanitarios, establecidas mediante la legislación nacional por la que se transpone la Directiva 95/46/CE o por decisión de la autoridad de control [1].

Con el fin de garantizar la calidad de los datos personales que se intercambian a través del sistema y, en particular, antes de enviar un mensaje selectivo, los usuarios del SAPR evaluarán si:

— los datos personales que quieren intercambiar son estrictamente necesarios para un procedimiento eficaz de trazabilidad de contactos. Es decir, la autoridad competente que envía el mensaje solo debe indicar a la del otro Estado miembro afectado los datos personales necesarios para identificar sin ambigüedad a las personas infectadas o expuestas al contagio. La lista indicativa de datos personales que pueden intercambiarse a efectos de la trazabilidad de los contactos, anexa a la Decisión 2009/547/CE, no debe equipararse a la concesión de una autorización general e incondicional para tratar dichas categorías de datos. Al mismo tiempo, hay que extremar precauciones en cuanto al tratamiento de datos personales no enumerados en dicho anexo, pues su difusión puede ser excesiva y poco razonable. En su lugar, hay que evaluar caso por caso si es estrictamente necesario incluir determinados datos personales a efectos de la trazabilidad de un contacto dado.

Tratamiento y almacenamiento de datos personales fuera del SAPR:

Es de capital importancia saber que la legislación nacional de protección de datos por la que se transpone la Directiva 95/46/CE también se aplica al almacenamiento y segundo tratamiento, fuera del SAPR, de los datos personales obtenidos a través del sistema. Esto puede ocurrir, por ejemplo, cuando los datos personales almacenados de forma centralizada por el sistema se guardan luego en ordenadores de usuarios o en bases de datos nacionales; o cuando la autoridad responsable de su tratamiento en el SAPR transmite esos datos a otras autoridades o a terceros. En estos casos, se recuerda a los usuarios del SAPR que:

— el almacenamiento y segundo tratamiento fuera del SAPR no han de ser incompatibles con los fines iniciales para los que se recabaron e intercambiaron los datos en el SAPR;

— el segundo tratamiento tiene que tener una base jurídica en la correspondiente legislación nacional sobre protección de datos; ha de ser necesario, adecuado, pertinente y no excesivo respecto a la finalidad original de su recogida en el SAPR;

— los datos deben estar actualizados y ser eliminados cuando ya no sean necesarios para los fines perseguidos con su segundo tratamiento;

— al tomar datos del SAPR y difundirlos, el responsable del tratamiento debe informar de ello a los interesados para garantizar el tratamiento leal, a menos que sea imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley (artículo 11, apartado 2, de la Directiva 95/46/CE). Dado que la comunicación a un tercero puede estar prescrita en la legislación de solo uno de los Estados miembros involucrados y, por tanto, no conocerse en otros lugares, se procurará informar de ello, aun cuando la comunicación constituya una obligación legal expresa.

7. CONDICIONES FAVORABLES PARA LA PROTECCIÓN DE DATOS

Se ha dotado al SAPR de ciertas características para mejorar el cumplimiento de los principios de protección de datos descritos en el punto 6 y para instar a los usuarios del SAPR a evaluar la cuestión de la protección de los datos cada vez que lo utilicen. Por ejemplo:

— en la página inicial de los mensajes del SAPR aparece visiblemente el aviso de que el canal de mensajes generales no debe usarse para la trazabilidad de contactos ni para transmitir otros datos personales, que podrían quedar a la vista de destinatarios distintos de los que necesitan acceder a ellos;

— el acceso a la información intercambiada en el sistema se ha modulado mediante diversos perfiles de usuario y creando canales de comunicación selectiva, con salvaguardias apropiadas para que se cumplan las normas de protección de datos;

[1] Artículo 8, apartado 4, de la Directiva 95/46/CE.

— en particular, el canal de mensajes selectivos del SAPR es exclusivo para el intercambio de datos personales entre los Estados miembros afectados. Su opción por defecto excluye a la Comisión y al ECDC de la lista de posibles destinatarios de mensajes selectivos que contengan datos personales ([1]);

— el sistema borra automáticamente todos los mensajes selectivos con datos personales doce meses después de su fecha de envío (para más detalles, véase el punto 11 sobre conservación de datos);

— los usuarios pueden rectificar o suprimir directamente, en cualquier momento, los mensajes selectivos con datos personales inexactos, no actualizados, ya no necesarios, o que no se atengan a las normas de protección de datos. Los demás usuarios del SAPR que participen en ese intercambio concreto de información selectiva reciben una notificación automática de que el mensaje ha sido eliminado, o modificado, en cumplimiento de las normas de protección de datos;

— en el canal de mensajería selectiva, las autoridades nacionales afectadas por un determinado intercambio de información pueden comunicarse y cooperar en cuanto a las peticiones de acceso, rectificación, bloqueo o supresión por parte de los interesados.

Además, a medio plazo está previsto integrar el módulo de formación del SAPR, de modo que los usuarios puedan consultar explicaciones exhaustivas sobre el funcionamiento del sistema, desde la perspectiva de la protección de datos. Con ejemplos prácticos se ilustrará la utilización de las diversas características y funcionalidades destinadas a mejorar el cumplimiento de las normas de protección de datos.

La Comisión tiene la intención de colaborar con los Estados miembros para garantizar que la «privacidad desde el diseño» sea el concepto rector de toda evolución futura del SAPR desde su concepción ([2]), y que se tengan en cuenta los principios de necesidad, proporcionalidad, limitación de la finalidad y recogida del mínimo de datos al decidir qué información puede intercambiarse por el SAPR, con quién y en qué condiciones.

8. COMUNICACIÓN DE INFORMACIÓN A LOS INTERESADOS

Uno de los principales requisitos del marco jurídico de la UE sobre protección de datos es la obligación de que el responsable del tratamiento de los datos suministre a los interesados información precisa sobre las operaciones de tratamiento de sus datos personales que se propone llevar a cabo.

Como coordinadora del SAPR y para cumplir su obligación ([3]), la Comisión ha colgado en su página web del SAPR una declaración de protección de la intimidad, clara y completa, relativa a las operaciones de tratamiento realizadas bajo responsabilidad de la propia Comisión y a las llevadas a cabo por las autoridades competentes, en particular en materia de trazabilidad de los contactos.

Sin embargo, la responsabilidad de comunicar información a los interesados también recae en las autoridades nacionales competentes en los Estados miembros, como responsables de sus respectivas operaciones de tratamiento en el marco del SAPR.

¿Qué «información» tienen que dar a los interesados las autoridades nacionales competentes del SAPR?

Cuando los datos se recaban del propio interesado, el artículo 10 de la Directiva 95/46/CE establece que el responsable del tratamiento o su representante deben comunicar al interesado, en el momento de recabar los datos, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

a) la identidad del responsable del tratamiento o, en su caso, de su representante;

([1]) No obstante, existe en el SAPR una opción alternativa para que los usuarios puedan utilizar también este canal selectivo para comunicarse información técnica sin transmisión de datos personales. Si se elige esta alternativa en vez de la opción por defecto, la autoridad que envía el mensaje puede poner a la Comisión y al ECDC como destinatarios. De este modo se tiene en cuenta el papel institucional de la Comisión para coordinar la gestión del riesgo y de incidentes, y el del ECDC para las tareas de evaluación del riesgo.

([2]) Según el principio de «privacidad desde el diseño», las tecnologías de la información y la comunicación tienen que diseñarse y desarrollarse teniendo en cuenta las normas de protección de los datos y de la intimidad desde su concepción y en todas las fases de su desarrollo.

([3]) La obligación de información incumbe a la Comisión a tenor de los artículos 11 y 12 del Reglamento (CE) nº 45/2001.

b) los fines del tratamiento de que van a ser objeto los datos;

c) cualquier otra información tal como:

— los destinatarios o las categorías de destinatarios de los datos,

— el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,

— la existencia de derechos de acceso y rectificación de los datos que le conciernen,

en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

El artículo 11 de la Directiva 95/46/CE enumera la información mínima que debe facilitar el responsable del tratamiento de los datos cuando estos no han sido recabados del propio interesado. Esta información debe comunicarse desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar en el momento de la primera comunicación de datos ([1]).

De estas disposiciones se desprende que las autoridades nacionales competentes deben dar directamente a los interesados un aviso jurídico con la información que figura en los artículos 10 y 11 de la Directiva 95/46/CE en el momento en que recaban sus datos personales (o, a más tardar, al comunicar por primera vez dichos datos a través del SAPR), a fin de que se adopten las medidas necesarias para proteger la salud pública frente a hechos de notificación obligatoria a tenor de la Decisión nº 2119/98/CE y sus disposiciones de aplicación. En el aviso figurará también una breve referencia al SAPR y un enlace a los correspondientes documentos y declaraciones de confidencialidad en los sitios web de las autoridades nacionales competentes, así como a la página web de la Comisión para el SAPR.

Los detalles concretos de la información que debe facilitar el aviso jurídico pueden diferir mucho de un Estado miembro a otro. Algunas legislaciones nacionales prevén que los responsables del tratamiento de datos ofrezcan obligatoriamente más información, como el derecho de los interesados a obtener reparación, el almacenamiento y conservación de los datos, las medidas de seguridad, etc.

Cierto es que la necesidad de intervenir a tiempo en situaciones de emergencia sanitaria puede impedir ofrecer a los interesados toda la información sobre los fines del tratamiento de sus datos personales, cuando no han sido recabados de los propios interesados. A este respecto, el artículo 11, apartado 2, de la Directiva 95/46/CE establece que podrá restringirse el derecho de información de los interesados «cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas».

De modo más general, cabe señalar que las legislaciones nacionales de protección de datos por las que se transpone la Directiva 95/46/CE pueden permitir determinadas restricciones o limitaciones del derecho a la información de los interesados ([2]). Tales limitaciones o restricciones nacionales específicas se mencionarán sin ambigüedades en los avisos de confidencialidad dirigidos a los interesados o publicados por las autoridades nacionales competentes en sus sitios web.

Las autoridades nacionales competentes de los Estados miembros deciden el modo y la manera de dar esa información a los interesados. Como la mayoría de las autoridades competentes realizará otras operaciones de tratamiento distintas del intercambio de información en el marco del SAPR, la forma de informar a las personas podrá ser, en su caso, la misma elegida para transmitir información similar en otras operaciones de tratamiento de datos con arreglo a la legislación nacional. Además, se recomienda que las autoridades nacionales competentes actualicen o complementen sus políticas o declaraciones de confidencialidad, si ya figuran en sus sitios web, con una referencia específica al intercambio de datos personales en el SAPR.

([1]) La información que debe facilitarse es la que figura en el mencionado artículo 10, a la que se añaden las categorías de los datos de que se trate. Obviamente, esta información no es obligatoria al recabar los datos directamente del interesado, que conoce las categorías de los datos en el momento en que se le preguntan.

([2]) El artículo 13, apartado 1, de la Directiva 95/46/CE, sobre excepciones y limitaciones, establece lo siguiente: «Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico o financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque solo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas».

Por todo lo dicho, es fundamental que las autoridades competentes de los Estados miembros consulten a su autoridad de control al redactar avisos jurídicos y declaraciones de confidencialidad, de conformidad con los artículos 10 y 11 de la Directiva 95/46/CE.

9. EL ACCESO A LOS DATOS PERSONALES Y OTROS DERECHOS DE LOS INTERESADOS

Las normas de protección de datos relativas a la comunicación de información a los interesados, presentadas en el punto 8, persiguen el objetivo de garantizar la transparencia de las operaciones de tratamiento de datos personales. La transparencia es también el objetivo subyacente de las disposiciones sobre los derechos de acceso de los interesados, establecidos en los instrumentos jurídicos de la UE al respecto ([1]).

¿Qué «derecho de acceso a los datos» tiene el interesado?

Los responsables del tratamiento de datos deben garantizar a todos los interesados el derecho a obtener, sin retrasos ni gastos excesivos, confirmación de si se están tratando datos personales que les conciernan, e información sobre la finalidad del tratamiento y sobre los posibles destinatarios de los datos.

Los responsables del tratamiento de datos deben también garantizar el derecho de los interesados a obtener la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a la legislación al respecto por ser, por ejemplo, incompletos o inexactos.

Por último, los responsables del tratamiento de datos tienen que notificar a los terceros a quienes se hayan comunicado los datos toda rectificación, supresión o bloqueo efectuados previa solicitud fundada del interesado, si no resulta imposible o supone un esfuerzo desproporcionado.

Como responsables del tratamiento, la Comisión y los Estados miembros comparten la responsabilidad de concesión de derechos de acceso, rectificación, bloqueo y supresión de datos personales tratados en el SAPR en los términos que se exponen a continuación.

La Comisión es responsable de otorgar acceso a los datos personales de los puntos de contacto nacionales del SAPR y de gestionar las correspondientes peticiones de rectificación, bloqueo y supresión. Se invita a los puntos de contacto nacionales a consultar la cláusula específica de la declaración general de confidencialidad en la página web de la Comisión para el SAPR ([2]) para información más detallada sobre cómo ejercer sus derechos como interesados.

Se comunica asimismo a los usuarios del SAPR que ya pueden modificar directamente sus datos personales. Sin embargo, los usuarios no pueden modificar directamente los campos en que se identifica una determinada cuenta del SAPR (dirección de correo electrónico acreditada, tipo de cuenta, etc.), para prevenir el riesgo de que usuarios no autorizados accedan al sistema. Por lo tanto, cualquier solicitud de modificación de estos campos de datos deberá dirigirse al responsable del tratamiento de datos en la Comisión, tal como se indica en la declaración general de confidencialidad en la página web de la Comisión para el SAPR.

La responsabilidad de tratar las solicitudes de los interesados sobre trazabilidad de contactos, datos de salud y otros datos personales intercambiados entre Estados miembros a través del SAPR recae en las autoridades competentes que intercambian los respectivos mensajes selectivos. Esta responsabilidad se rige por las disposiciones pertinentes de la legislación nacional en materia de protección de datos por la que se transpone la Directiva 95/46/CE.

Sin embargo, cabe señalar que las disposiciones pertinentes de la legislación nacional en materia de protección de datos por la que se transpone la Directiva 95/46/CE pueden establecer restricciones o limitaciones específicas al derecho de acceso, rectificación, supresión o bloqueo de los datos de los interesados ([3]). Tales limitaciones o restricciones se mencionarán sin ambigüedades en los avisos de confidencialidad dirigidos a los interesados o publicados por las autoridades nacionales competentes en sus sitios web. Por tanto, se aconseja a los puntos de contacto del SAPR que consulten a su autoridad de control para obtener más información al respecto.

La complejidad del SAPR, con participación de muchos usuarios en operaciones conjuntas de tratamiento, requiere un enfoque claro y sencillo del derecho de acceso a los datos de los propios interesados, que, aun no estando familiarizados con el funcionamiento del sistema, deben poder ejercer de manera efectiva sus derechos.

([1]) Artículo 12 de la Directiva 95/46/CE y artículos 13 a 18 del Reglamento (CE) nº 45/2001.
([2]) Todos los usuarios del SAPR pueden consultar también la declaración de confidencialidad en la sección protegida de la aplicación.
([3]) Artículo 13, apartado 1, de la Directiva 95/46/CE.

Se recomienda que si un interesado cree que sus datos personales están siendo tratados en el SAPR y desea acceder a ellos, eliminarlos o rectificarlos, pueda dirigirse a cualquiera de las autoridades nacionales competentes con las que ha tenido contacto o que recabaron sus datos en relación con un hecho específico que presenta un riesgo para la salud pública (por ejemplo, la autoridad del país del que es ciudadano y la del país de estancia cuando se produjo el incidente), así como a cualquier otra autoridad implicada en el intercambio de información relacionada con la aplicación de medidas de trazabilidad de los contactos.

Ninguna autoridad involucrada en dicho intercambio de información podrá denegar el derecho de acceso, rectificación o supresión alegando que no fue ella la que introdujo los datos en el SAPR, o que el interesado debe ponerse en contacto con otra autoridad competente. En particular, si la petición del interesado la recibe una autoridad competente distinta de la que envió la información original por el canal de mensajes selectivos, es esta autoridad receptora quien debe remitir la solicitud, a través del mecanismo específico mencionado en el punto 7, a la autoridad competente que envió el mensaje original, para que esta tome una decisión al respecto.

Si procede, antes de adoptar una decisión, la autoridad competente que lanzó la información podrá ponerse en contacto con otras autoridades competentes que participen en el intercambio de información, o afectadas de otro modo por la solicitud del interesado, a través del mecanismo específico mencionado en el punto 7.

También hay que comunicar a los interesados que, si no están satisfechos con la respuesta recibida, pueden dirigirse a otra autoridad competente involucrada en el intercambio de información. En cualquier caso, los interesados tienen derecho a presentar una queja ante la autoridad de control de una de las autoridades competentes involucradas, la que consideren más conveniente. Si es procedente y necesario, las autoridades de control cooperarán para resolver la queja (véase el artículo 28 de la Directiva 95/46/CE).

Por último, de resultas de una recomendación específica del SEPD en su dictamen, la Comisión ha añadido al SAPR la posibilidad de rectificar y suprimir, a efectos de protección de datos, mensajes selectivos con datos personales inexactos, no actualizados, ya no necesarios, o que no se atengan a las normas de protección de datos.

10. SEGURIDAD DE LOS DATOS

El acceso al sistema está limitado a usuarios autorizados de la Comisión, del ECDC y de los puntos nacionales de contacto del SAPR formalmente designados. El acceso está protegido mediante cuentas de usuario y contraseñas protegidas y personalizadas.

Los procedimientos para tratar datos personales en el SAPR están establecidos con referencia a las disposiciones de los artículos 21 y 22 del Reglamento (CE) nº 45/2001.

11. CONSERVACIÓN DE LOS DATOS

De conformidad con los requisitos de protección de datos establecidos en el artículo 4, apartado 1, letra e), del Reglamento (CE) nº 45/2001 y en el artículo 6, apartado 1, letra e), de la Directiva 95/46/CE, el sistema borrará automáticamente todos los mensajes selectivos con datos personales doce meses después de su fecha de envío.

No obstante, esta salvaguardia intrínseca del sistema no dispensa a los usuarios —que son individualmente los responsables únicos de los datos que tratan en el canal de mensajes selectivos— de adoptar medidas para eliminar de la red los datos personales que hayan dejado de ser necesarios antes de la expiración de ese plazo de doce meses.

Con este fin, la Comisión ha introducido en el SAPR una nueva aplicación gracias a la cual los usuarios pueden suprimir directamente, en cualquier momento, los mensajes selectivos con datos personales ya innecesarios.

Por último, conviene recordar que, en cuanto a la conservación de los datos, las autoridades nacionales competentes tienen que cumplir sus propias normas de protección de datos personales, establecidas en la legislación nacional por la que se transpone la Directiva 95/46/CE. El borrado automático al cabo de un año de la información personal almacenada en el sistema no impide a los usuarios almacenar la misma información fuera del SAPR durante un lapso de tiempo diferente (por ejemplo, más largo), si respetan lo establecido en sus respectivas normativas nacionales sobre protección de datos, y siempre que los plazos previstos en la legislación nacional sean compatibles con lo dispuesto en el artículo 6, apartado 1, letra e), de la Directiva 95/46/CE.

12. COOPERACIÓN CON LAS AUTORIDADES NACIONALES DE PROTECCIÓN DE DATOS

Se recomienda a las autoridades competentes consultar con sus respectivas autoridades nacionales de control, especialmente en cuestiones de protección de datos no cubiertas por las presentes directrices.

También deben saber las autoridades competentes que, en función de las disposiciones de la legislación nacional por la que se transpone la Directiva 95/46/CE, pueden tener que notificar a las respectivas autoridades de control sus propias actividades de tratamiento de datos en el SAPR. Incluso puede ser necesaria, en algunos Estados miembros, la autorización previa de las autoridades de control.