COMISIÓN EUROPEA

Bruselas, 25.1.2012
COM(2012) 10 final

2012/0010 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos

[…]

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

La presente exposición de motivos presenta en detalle el enfoque del nuevo marco jurídico para la protección de los datos personales en la UE como se establece en la Comunicación COM (2012) 9 final. El marco jurídico consta de dos propuestas legislativas:

– una propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), y

– una propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y a la libre circulación de estos datos.

La presente exposición de motivos se refiere a esta última propuesta legislativa.

La piedra angular de la legislación vigente de la UE en materia de protección de datos, la Directiva 95/46/CE[1], fue adoptada en 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de datos personales entre los Estados miembros. Se complementó con varios instrumentos que establecen normas específicas sobre protección de datos en el ámbito de la cooperación policial y judicial en materia penal[2] (antiguo tercer pilar), incluida la Decisión Marco 2008/977/JAI[3].

El Consejo Europeo invitó a la Comisión a evaluar el funcionamiento de los instrumentos de la UE en materia de protección de datos y a presentar, en caso necesario, nuevas iniciativas legislativas y no legislativas[4]. En su resolución sobre el Programa de Estocolmo, el Parlamento Europeo[5] acogió favorablemente un régimen general de protección de datos en la UE y, entre otras cosas, abogó por la revisión de la Decisión Marco. En su Plan de acción por el que se aplica el programa de Estocolmo[6], la Comisión subrayó la necesidad de garantizar que el derecho fundamental a la protección de datos de carácter personal se aplique de forma coherente en el contexto de todas las políticas de la UE. El Plan de Acción subrayaba que «en una sociedad global caracterizada por la rapidez del cambio tecnológico, donde el intercambio de información no conoce fronteras, es especialmente importante proteger la intimidad. La Unión debe garantizar la aplicación coherente del derecho fundamental a la protección de datos. Debemos reforzar la posición de la UE en cuanto a la protección de los datos

---

1 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, DO L 281 de 23.11.1995, p. 31.

2 Véase la lista completa en el anexo 3 de la evaluación de impacto (SEC (2012) 72).

3 Decisión Marco 2008/977/JAI, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO L 350 de 30.12.2008, p. 60.

4 En el Programa de Estocolmo, DO C 115 de 4.5.2010, p. 1.

5 Véase la Resolución del Parlamento Europeo sobre el Programa de Estocolmo, adoptada el 25 de noviembre de 2009.

6 COM (2010) 171final.

personales en el contexto de todas las políticas de la UE, incluida la represión policial y la prevención de la delincuencia, así como en nuestras relaciones internacionales.».

En su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea»[7], la Comisión concluyó que la UE necesita una política más integradora y coherente en materia del derecho fundamental de la protección de datos de carácter personal.

La Decisión Marco 2008/977/JAI tiene un ámbito de aplicación limitado, ya que solo se aplica al tratamiento transfronterizo de datos y no a las actividades de tratamiento por parte de las autoridades policiales y judiciales a nivel puramente nacional. Ello puede crear dificultades a las autoridades policiales y otras autoridades competentes en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial. No son siempre capaces de distinguir fácilmente entre el tratamiento meramente nacional y el transfronterizo no de prever si determinados datos personales pueden convertirse en objeto de un intercambio transfronterizo en una fase posterior (véase la sección 2). Además, por su naturaleza y contenido, la Decisión Marco deja un amplio margen de maniobra a los Estados miembros para transponer sus disposiciones de Derecho interno. Por otra parte, no contiene ningún mecanismo o grupo consultivo similar al Grupo del artículo 29 que sustente una interpretación común de sus disposiciones, ni establece competencias de ejecución de la Comisión a fin de garantizar un enfoque común en su aplicación.

El artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establece el principio según el cual toda persona tiene derecho a la protección de los datos de carácter personal. Además, con el artículo 16, apartado 2, del TFUE, el Tratado de Lisboa introduce una base jurídica específica para la adopción de normas relativas a la protección de los datos personales que también se aplica a la cooperación judicial en materia penal y la cooperación policial. El artículo 8 de la Carta de los Derechos Fundamentales de la UE consagra como derecho fundamental la protección de los datos personales. El artículo 16 del TFUE obliga al legislador a establecer normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, también en los ámbitos de la cooperación judicial en materia penal y la cooperación policial, que comprende tanto el tratamiento de datos personales transfronterizo como el nacional. Ello permitirá que se protejan los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, garantizando al mismo tiempo el intercambio de datos personales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. Todo ello contribuirá a facilitar la cooperación en el ámbito de la lucha contra la delincuencia en Europa.

Debido a la naturaleza específica del ámbito de la cooperación policial y judicial en materia penal, en la Declaración 21[8] se reconoció que podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 del TFUE.

---

7 Comunicación de la Comisión Europea «Un enfoque global de la protección de los datos personales en la Unión Europea», COM (2010) 609 final de 4 de noviembre de 2010.

8 Declaración 21, relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial (aneja al Acta final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa, 13.12.2007).

2. RESULTADOS DE LA CONSULTA DE LAS PARTES INTERESADAS Y EVALUACIÓN DE IMPACTO

Esta iniciativa es el resultado de una amplia consulta con todas las partes interesadas sobre la revisión del actual marco jurídico para la protección de datos de carácter personal, que incluyó dos fases de consulta pública:

– Del 9 de julio al 31 de diciembre de 2009, la *Consulta sobre el marco jurídico para el derecho fundamental a la protección de datos de carácter personal*. La Comisión recibió 168 respuestas, 127 de personas físicas, organizaciones y asociaciones empresariales, y 12 de autoridades públicas. Las respuestas no confidenciales pueden consultarse en el sitio internet de la Comisión[9].

– Del 4 de noviembre de 2010 al 15 de enero de 2011, la *Consulta sobre el enfoque global de la Comisión sobre la protección de datos de carácter personal en la Unión Europea*. La Comisión recibió 305 respuestas, de las cuales 54 procedían de ciudadanos, 31 de autoridades públicas y 220 de organizaciones privadas, especialmente de asociaciones empresariales y organizaciones no gubernamentales. Las respuestas no confidenciales pueden consultarse en el sitio internet de la Comisión[10].

Habida cuenta de que dichas consultas se centraron en gran medida en la revisión de la Directiva 95/46/CE, se llevaron a cabo consultas específicas con los servicios con funciones coercitivas; en particular, el 29 de junio de 2010 se organizó un seminario con las autoridades de los Estados miembros sobre la aplicación de las normas de protección de datos a las autoridades públicas, incluso en el ámbito de la cooperación judicial en materia penal y la cooperación policial. Además, el 2 de febrero de 2011, la Comisión convocó un seminario con las autoridades de los Estados miembros para debatir sobre la aplicación de la Decisión Marco 2008/977/JAI del Consejo y, más en general, cuestiones de protección de datos en el ámbito de la cooperación judicial en materia penal y la cooperación policial.

Se consultó a los ciudadanos de la UE mediante un Eurobarómetro realizado en noviembre-diciembre de 2010[11]. También se pusieron en marcha varios estudios[12]. El «Grupo del Artículo 29»[13] emitió varios dictámenes y presentó observaciones útiles a la Comisión[14]. El

---

9 http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

10 http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

11 Eurobarómetro espacial (EB) 359, *Data Protection and Electronic Identity in the EU* (Protección de datos e identidad electrónica en la UE, 2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

12 Véase el *Estudio sobre las ventajas económicas de las tecnologías potenciadoras de la privacidad* o el *Estudio comparativo de los distintos enfoques ante los nuevos retos en materia de protección de la privacidad, en particular a la luz de los avances tecnológicos*, enero de 2010. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf).

13 Este grupo de trabajo se creó en 1996 (por el artículo 29 de la Directiva) con carácter consultivo y estaba compuesto por representantes de las autoridades nacionales de protección de datos (DPA), el Supervisor Europeo de Protección de Datos (SEPD) y la Comisión. Para consultar información adicional sobre sus actividades, véase http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

14 Véanse, en particular, los siguientes dictámenes: sobre «El futuro de la intimidad» (2009, WP 168); sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (1/2010, WP 169); sobre la publicidad del comportamiento en línea (2/2010, WP 171); sobre el principio de la obligación de rendir cuentas (3/2010, WP 173); sobre la legislación aplicable (8/2010, WP 179); y sobre el consentimiento (15/2011, WP 187). A petición de la Comisión, también adoptó los tres documentos de

Supervisor Europeo de Protección de Datos también emitió un dictamen general sobre los temas planteados en la Comunicación de la Comisión de noviembre de 2010[15].

Mediante su Resolución de 6 de julio de 2011 el Parlamento Europeo aprobó un informe que respaldaba el planteamiento de la Comisión para reformar el marco de la protección de datos[16]. El 24 de febrero de 2011, el Consejo de la Unión Europea adoptó las conclusiones en las que respalda en términos generales la intención de la Comisión de reformar el marco de la protección de datos, y concuerda con muchos elementos del planteamiento de la Comisión. El Comité Económico y Social Europeo también apoyó el impulso general de la Comisión destinado a garantizar una aplicación más coherente de las normas de protección de datos de la UE en todos los Estados miembros y una revisión adecuada de la Directiva 95/46/CE[17].

De conformidad con su política «Legislar mejor», la Comisión realizó una evaluación de impacto de distintas posibilidades de actuación[18]. La evaluación de impacto se basó en tres objetivos estratégicos: mejorar la dimensión de mercado interior de la protección de datos, hacer más efectivo el ejercicio de los derechos de protección de datos por los ciudadanos y crear un marco global y coherente que abarque todos los ámbitos de competencia de la Unión, incluida la cooperación policial y judicial en materia penal. Respecto a este último objetivo en particular, se evaluaron dos opciones estratégicas: una primera que básicamente amplía el ámbito de aplicación de las normas de protección de datos en este campo y aborda las carencias y otras cuestiones planteadas por la Decisión Marco, y una segunda de mayor alcance, con normas muy prescriptivas y estrictas, que también entrañaría la modificación inmediata de todos los demás instrumentos del «antiguo tercer pilar». Una tercera opción «minimalista», basada en gran medida en comunicaciones interpretativas y en medidas de apoyo político, tales como programas de financiación y herramientas técnicas, con una mínima intervención legislativa, no se consideró apropiada para tratar las cuestiones señaladas en este ámbito en relación con la protección de datos.

Con arreglo a la metodología consolidada de la Comisión, cada opción fue evaluada, con ayuda de un grupo director interservicios, en función de su efectividad a la hora de alcanzar los objetivos estratégicos, su impacto económico en los interesados (también sobre el presupuesto de las instituciones de la UE), su impacto social y su incidencia en los derechos fundamentales. No se examinó el impacto en el medio ambiente.

El análisis del impacto global llevó al desarrollo de la opción estratégica preferida, que se ha incorporado en la presente propuesta. Según la evaluación, su ejecución conducirá a un mayor refuerzo de la protección de datos en este ámbito, mediante la inclusión, en particular, del tratamiento de datos a escala nacional, gracias a lo cual también se logrará una mayor seguridad jurídica para las autoridades competentes en los ámbitos de la cooperación judicial en materia penal y la cooperación policial.

---

orientación siguientes: sobre notificaciones, datos sensibles y la aplicación práctica del artículo 28, apartado 6, de la Directiva 95/46/CE. Todos ellos pueden consultarse en: http://ec.europa.eu/justice/protección de datos/article-29/documentation/index_en.htm.

15 Puede consultarse en el sitio internet del SEPD: http://www.edps.europa.eu/EDPSWEB/.

16 Resolución del PE de 6 de julio de 2011 sobre un enfoque global de la protección de los datos personales en la Unión Europea (2011/2025(INI), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&language=EN&ring=A7-2011-0244 (ponente: MEP Axel Voss (PPE/DE).

17 CESE 999/2011.

18 SEC(2012) 72.

El 9 de septiembre de 2011, el Comité de Evaluación de Impacto (CEI) emitió un dictamen sobre el proyecto de evaluación de impacto. A raíz del dictamen del CEI, se introdujeron en la evaluación de impacto, entre otros, los cambios siguientes:

– se aclararon los objetivos del marco jurídico en vigor (en qué medida se alcanzaron y en qué medida no se lograron), y los objetivos de la reforma prevista;

– en la sección consagrada a la definición de problemas se añadieron más elementos de prueba y explicaciones/aclaraciones adicionales.

La Comisión elaboró también un informe de ejecución relativo a la Decisión Marco 2008/977/JAI, basado en su artículo 29, apartado 2, que se ha de adoptar formando parte del presente paquete de protección de datos[19]. Las conclusiones del informe, que se basa en las aportaciones realizadas por los Estados miembros, también se incluyeron en la preparación de la evaluación de impacto.

3. ASPECTOS JURÍDICOS DE LA PROPUESTA

3.1. Base jurídica

La propuesta se basa en el artículo 16, apartado 2, del TFUE, que es una nueva base jurídica específica introducida por el Tratado de Lisboa para la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos, y por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y de normas relativas a la libre circulación de estos datos.

La propuesta tiene por objeto garantizar un nivel uniforme y elevado de protección de los datos en este ámbito, reforzando así la confianza mutua entre las autoridades policiales y judiciales de los distintos Estados miembros y facilitando la libre circulación de datos y la cooperación entre las autoridades policiales y judiciales.

3.2. Subsidiariedad y proporcionalidad

Con arreglo al principio de subsidiariedad (artículo 5, apartado 3, del TUE), la Unión solo debe intervenir en caso de que los objetivos perseguidos no puedan ser alcanzados de manera suficiente por los Estados miembros por sí solos, sino que puedan alcanzarse mejor, debido a la dimensión o a los efectos de la acción pretendida, a escala de la Unión. A la luz de los problemas esbozados anteriormente, el análisis de subsidiariedad indica la necesidad de adoptar iniciativas a escala de la UE en los ámbitos policial y de justicia penal por las razones siguientes:

– El derecho a la protección de datos de carácter personal, consagrado en el artículo 8 de la Carta de los Derechos Fundamentales y en el artículo 16, apartado 1, del TFUE, requiere el mismo nivel de protección de datos en toda la Unión. Requiere el mismo nivel de protección para los datos intercambiados y los datos tratados a escala nacional.

[19] COM(2012) 12.

– Existe una necesidad creciente de que los servicios con funciones coercitivas de los Estados miembros sometan a tratamiento e intercambien datos a velocidades cada vez mayores con el fin de prevenir y luchar contra el terrorismo y la delincuencia transnacionales. En este contexto, la existencia de normas claras y coherentes en materia de protección de datos a escala de la UE ayudará a fomentar la cooperación entre dichas autoridades.

– Además, existen retos prácticos a la ejecución de la legislación de protección de datos y la necesidad de cooperación entre los Estados miembros y sus autoridades, que tiene que organizarse a escala de la UE para garantizar la aplicación uniforme del Derecho de la Unión. En determinadas situaciones, la UE es la que está en mejores condiciones para garantizar de forma efectiva y coherente el mismo nivel de protección de los ciudadanos cuando sus datos personales se transfieren a terceros países.

– Por sí solos los Estados miembros no pueden mitigar los problemas que se plantean en la situación actual, especialmente los debidos a la fragmentación de las legislaciones nacionales. Por tanto, existe una necesidad específica de establecer un marco armonizado y coherente que permita una adecuada transferencia de datos personales a través de las fronteras interiores de la UE, al tiempo que se garantiza una protección efectiva a todas las personas físicas en la UE.

– Es probable que las iniciativas legislativas de la UE propuestas sean más efectivas que acciones similares adoptadas a nivel de los Estados miembros debido a la naturaleza y magnitud de los problemas, que no se circunscriben al ámbito de uno o varios Estados miembros.

El principio de proporcionalidad requiere que cualquier intervención tenga una finalidad específica y no vaya más allá de lo necesario para alcanzar sus objetivos. Este principio ha servido de guía en la elaboración de la presente propuesta, desde la identificación y evaluación de las opciones políticas alternativas a la redacción de la propuesta legislativa.

La Directiva es, por consiguiente, el mejor instrumento para garantizar en este ámbito la armonización a nivel de la UE y dejar, al mismo tiempo, a los Estados miembros la flexibilidad necesaria a la hora de aplicar los principios, las normas y sus exenciones a nivel nacional. Dada la complejidad de las normas nacionales vigentes relativas a la protección de datos personales tratados en el ámbito de la cooperación policial y la cooperación judicial en materia penal, y habida cuenta del objetivo de armonización global de estas normas por medio de la presente Directiva, la Comisión tendrá que solicitar a los Estados miembros que faciliten documentos explicativos que aclaren la relación existente entre los componentes de la Directiva y las partes correspondientes de los instrumentos nacionales de transposición, a fin de poder llevar a cabo su tarea de supervisión de la transposición de la presente Directiva.

3.3. Resumen de las cuestiones relativas a los derechos fundamentales

El derecho a la protección de los datos de carácter personal se establece en el artículo 8 de la Carta de los Derechos Fundamentales de la UE, en el artículo 16 del TFUE y en el artículo 8 del CEDH. Como subrayó el Tribunal de Justicia de la UE[20], el derecho a la protección de datos de carácter personal no es un derecho absoluto, sino que se ha de considerar en relación

[20] Tribunal de Justicia de la Unión Europea, sentencia de 9.11.2010, asuntos acumulados C-92/09 y C-93/09 Volker und Markus schecke y Eifert [Rec. 2010, p. I-0000).

con su función en la sociedad[21]. La protección de datos está estrechamente vinculada al respeto de la vida privada y familiar establecido en el artículo 7 de la Carta. Ello se refleja en el artículo 1, apartado 1, de la Directiva 95/46/CE, que establece que los Estados miembros garantizarán la protección de las libertades y de los derechos fundamentales de las personas físicas, y en particular del derecho a la intimidad, en lo que respecta al tratamiento de datos personales.

Otros derechos fundamentales potencialmente afectados y consagrados en la Carta son la prohibición de cualquier tipo de discriminación, y en particular la ejercida por razón de raza, orígenes étnicos, características genéticas, religión o convicciones, opiniones políticas o de cualquier otro tipo, discapacidad u orientación sexual (artículo 21); los derechos del niño (artículo 24) y el derecho a la tutela judicial efectiva y a un juez imparcial (artículo 47).

3.4. Exposición detallada de la propuesta

3.4.1. CAPÍTULO I – DISPOSICIONES GENERALES

El artículo 1 define el objeto de la Directiva, es decir, las normas relativas al tratamiento de datos personales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y fija el doble objetivo de la Directiva, a saber, proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, al tiempo que se garantiza un alto nivel de seguridad pública, y asegurar el intercambio de datos personales entre las autoridades competentes dentro de la Unión.

El artículo 2 define el ámbito de aplicación de la Directiva, que no se limita al tratamiento transfronterizo de datos, sino que se aplica a todas las operaciones de tratamiento efectuadas por «autoridades competentes» (tal como se definen en el artículo 3, apartado 14), a los efectos de la Directiva. La Directiva no se aplica ni al tratamiento en el ejercicio de una actividad que no esté comprendida en el ámbito de aplicación del Derecho de la Unión, ni a las operaciones de tratamiento efectuadas por instituciones, órganos y organismos de la Unión, que están sujetas al Reglamento (CE) nº 45/2001 y otras normas específicas.

El artículo 3 incluye las definiciones de los términos utilizados en la Directiva. Mientras que algunas definiciones se han tomado de la Directiva 95/46/CE y la Decisión Marco 2008/977/JAI, otras se modifican, complementadas con elementos adicionales o nuevos. Los nuevos conceptos son los de «violación de datos personales», «datos genéticos» y «datos biométricos», «autoridades competentes» [sobre la base del artículo 87, del TFUE y el artículo 2, letra h), de la Decisión Marco 2008/977/JAI], y «niño», basado en la Convención de las Naciones Unidas sobre los Derechos del Niño[22].

---

[21] En consonancia con el artículo 52, apartado 1, de la Carta, pueden introducirse limitaciones al ejercicio del derecho a la protección de datos, siempre que tales limitaciones estén establecidas por ley, respeten el contenido esencial de dichos derechos y libertades y, respetando el principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

[22] Mencionado también en el artículo 2, letra a), de la Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, DO L 335, 17.12.2011, p. 1.

3.4.2. *CAPÍTULO II - PRINCIPIOS*

El artículo 4 establece los principios relativos al tratamiento de datos personales, inspirándose en el artículo 6 de la Directiva 95/46/CE y en el artículo 3 de la Decisión Marco 2008/977/JAI, aunque adaptándolos al contexto específico de la presente Directiva.

El artículo 5 exige la distinción, en la medida de lo posible, entre datos de carácter personal de diferentes categorías de interesados. Se trata de una nueva disposición, que no figura ni en la Directiva 95/46/CE ni en la Decisión Marco 2008/977/JAI, pero que había sido propuesta por la Comisión en su propuesta original en relación con la Decisión Marco[23]. Está inspirada en la Recomendación del Consejo de Europa R (87) 15. Ya existen normas similares para Europol[24] y Eurojust[25].

El artículo 6 sobre los diferentes grados de precisión y fiabilidad refleja el principio 3.2 de la Recomendación del Consejo de Europa R (87) 15. Existen normas similares para Europol, también incluidas en la propuesta de la Comisión relativa a la Decisión Marco[26].

El artículo 7 establece los fundamentos para el tratamiento lícito, cuando resulte necesario para la ejecución de una tarea realizada por una autoridad competente, sobre la base de la legislación nacional, para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, con el fin de proteger los intereses vitales del interesado o de otra persona, o para evitar una amenaza inminente y grave para la seguridad pública. Los demás fundamentos para el tratamiento lícito que figuran en el artículo 7 de la Directiva 95/46/CE no son adecuados para el tratamiento en los ámbitos policial y de la justicia penal.

El artículo 8 establece una prohibición general del tratamiento de categorías especiales de datos personales y las excepciones a esta norma general, inspirándose en el artículo 8 de la Directiva 95/46/CE y añadiendo los datos genéticos, a raíz de la jurisprudencia del Tribunal Europeo de Derechos Humanos[27].

El artículo 9 establece la prohibición de las medidas basadas únicamente en el tratamiento automático de datos personales si no se autorizan por ley, ofreciendo las garantías apropiadas, de conformidad con el artículo 7 de la Decisión Marco 2008/977/JAI.

3.4.3. *CAPÍTULO III – DERECHOS DEL INTERESADO*

El artículo 10 introduce la obligación de los Estados miembros de ofrecer información de fácil acceso y comprensión, inspirada especialmente en el principio 10 de la Resolución de Madrid relativa a estándares internacionales sobre protección de datos personales y privacidad[28], y obliga a los responsables del tratamiento a establecer procedimientos y mecanismos para facilitar el ejercicio de los derechos del interesado. Ello incluye la obligación de que el ejercicio de los derechos sea en principio gratuito.

---

23 COM(2005) 475 final.

24 Artículo 14 de la Decisión 2009/371/JAI por la que se crea la Oficina Europea de Policía (Europol).

25 Artículo 15 de la Decisión 2009/426/JAI por la que se refuerza Eurojust.

26 Artículo 14 de la Decisión 2009/371/JAI por la que se crea la Oficina Europea de Policía (Europol).

27 Tribunal Europeo de Derechos Humanos, sentencia de 4.12.2008, S. y Marper / Reino Unido (nº demanda 30562/04 y 30566/04).

28 Adoptada por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de 5.11.2009.

En el artículo 11 se especifica la obligación de los Estados miembros de garantizar la información al interesado. Estas obligaciones se fundamentan en los artículos 10 y 11 de la Directiva 95/46/CE, sin que distintos artículos distingan si la información se recoge del interesado o no, y ampliando el espectro de la información que se ha de facilitar. Este artículo establece excepciones a la obligación de informar, cuando tales excepciones sean proporcionadas y necesarias en una sociedad democrática para el ejercicio de las tareas de las autoridades competentes (de conformidad con el artículo 13 de la Directiva 95/46/CE y el artículo 17 de la Decisión Marco 2008/977/JAI).

El artículo 12 establece la obligación de los Estados miembros de garantizar el derecho del interesado a acceder a sus datos personales. Se inspira en el artículo 12, letra a), de la Directiva 95/46/CE, añadiendo nuevos elementos para la información de los interesados (relativos al periodo de conservación, sus derechos de rectificación, supresión o restricción y a presentar una reclamación).

El artículo 13 establece que los Estados miembros podrán adoptar medidas legislativas que restrinjan el derecho de acceso, si así lo exige la naturaleza específica del tratamiento de datos en los ámbitos policial y de la justicia penal, y sobre la información del interesado relativa a una restricción de acceso, de conformidad con el artículo 17, apartados 2 y 3, de la Decisión Marco 2008/977/JAI.

El artículo 14 dispone que, cuando se restrinja el acceso directo, el interesado debe ser informado de la posibilidad de recurrir al acceso indirecto a través de la autoridad de control, que debe ejercer el derecho en su nombre y ha de informar al interesado del resultado de sus verificaciones.

El artículo 15 sobre el derecho de rectificación se inspira en el artículo 12, letra b), de la Directiva 95/46/CE; y, por lo que se refiere a las obligaciones en caso de denegación, en el artículo 18, apartado 1, de la Decisión Marco 2008/977/JAI.

El artículo 16 sobre el derecho de supresión se inspira en el artículo 12, letra b), de la Directiva 95/46/CE y, por lo que se refiere a las obligaciones en caso de denegación, en el artículo 18, apartado 1, de la Decisión Marco 2008/977/JAI. Este artículo integra también el derecho a que se marque el tratamiento en determinados casos, sustituyendo el término ambiguo «bloqueo», utilizado en el artículo 12, letra b), de la Directiva 95/46/CE y en el artículo 18, apartado 1, de la Decisión Marco 2008/977/JAI.

El artículo 17 sobre la rectificación, supresión y restricción del tratamiento en los procedimientos judiciales aporta precisiones sobre la base del artículo 4, apartado 4, de la Decisión Marco 2008/977/JAI.

3.4.4. CAPÍTULO IV – RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

3.4.4.1. SECCIÓN 1 - OBLIGACIONES GENERALES

El artículo 18 describe la obligación del responsable del tratamiento de ajustarse a lo establecido en la presente Directiva y garantizar su cumplimiento, incluida la adopción de políticas y mecanismos a tal efecto.

El artículo 19 establece que los Estados miembros deben velar por que el responsable del tratamiento cumpla las obligaciones que emanan de los principios de la protección de datos desde el diseño y por defecto.

El artículo 20 relativo a los corresponsables del tratamiento aclara su situación por lo que respecta a su relación interna.

El artículo 21 aclara la posición y la obligación de los encargados del tratamiento, inspirándose en parte en el artículo 17, apartado 2, de la Directiva 95/46/CE, y añadiendo nuevos elementos, incluido que un encargado que trate datos más allá de las instrucciones del responsable del tratamiento ha de ser considerado corresponsable.

El artículo 22, relativo al tratamiento efectuado bajo la autoridad del responsable y el encargado del tratamiento, se inspira en el artículo 16 de la Directiva 95/46/CE.

El artículo 23 introduce la obligación de que los responsables y encargados del tratamiento conserven la documentación de todos los sistemas y procedimientos de tratamiento que estén bajo su responsabilidad.

El artículo 24 se refiere a la conservación de registros, de conformidad con el artículo 10, apartado 1, de la Decisión Marco 2008/977, al tiempo que aporta nuevas precisiones.

El artículo 25 aclara las obligaciones del responsable y del encargado del tratamiento en relación con la cooperación con la autoridad de control.

El artículo 26 se refiere a los casos en que es obligatorio consultar a la autoridad de control antes del tratamiento, inspirado en el artículo 23 de la Decisión Marco 2008/977/JAI.

3.4.4.2. SECCIÓN 2 - SEGURIDAD DE LOS DATOS

El artículo 27, relativo a la seguridad del tratamiento, se inspira en el actual artículo 17, apartado 1, de la Directiva 95/46/CE, relativo a la seguridad del tratamiento, y en el artículo 22 de la Decisión Marco 2008/977/JAI, por el que se amplían las obligaciones correspondientes a los encargados del tratamiento, con independencia de su contrato con el responsable del tratamiento.

Inspirados en la notificación de la violación de datos personales contemplada en el artículo 4, apartado 3, de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, los artículos 28 y 29 introducen la obligación de notificar las violaciones de datos personales, aclarando y separando las obligaciones de notificar a la autoridad de control (artículo 28) y de comunicar, en determinadas circunstancias, al interesado (artículo 29). El artículo 29 establece también exenciones haciendo referencia al artículo 11, apartado 4.

3.4.4.3. SECCIÓN 3 - DELEGADO DE PROTECCIÓN DE DATOS

El artículo 30 introduce la obligación para el responsable del tratamiento de designar obligatoriamente a un delegado de protección de datos que debe cumplir las tareas que figuran en el artículo 32. Cuando varias autoridades competentes actúen bajo la supervisión de una autoridad central que opere en calidad de responsable del tratamiento, al menos esta autoridad central debe designar a un delegado de protección de datos. El artículo 18, apartado 2, de la Directiva 95/46/CE contemplaba la posibilidad de que los Estados miembros introdujesen tal requisito en lugar de la obligación de notificación general establecida en dicha Directiva.

El artículo 31 establece la función del delegado de protección de datos.

El artículo 32 establece las tareas del delegado de protección de datos.

3.4.5. *CAPÍTULO V – TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES*

El artículo 33 establece los principios generales para las transferencias de datos a terceros países u organizaciones internacionales en el ámbito de la cooperación policial y la cooperación judicial en materia penal, incluidas las transferencias ulteriores. Este artículo aclara que las transferencias a terceros países sólo podrán llevarse a cabo si son necesarias para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.

El artículo 34 establece que se pueden realizar transferencias a cualquier tercer país en relación con el cual la Comisión haya adoptado una decisión de adecuación, con arreglo al Reglamento …./../201X o, más específicamente, en el ámbito de la cooperación policial y la cooperación judicial en materia penal, o, en ausencia de tales decisiones, cuando se den las garantías apropiadas. Mientras no existan decisiones de adecuación, la Directiva garantiza que las transferencias pueden seguir llevándose a cabo, siempre que existan las garantías y excepciones adecuadas. Además, la Directiva fija los criterios que deberán tenerse en cuenta para que la Comisión evalúe si existe o no un nivel adecuado de protección y entre ellos se incluyen expresamente el Estado de Derecho, el recurso jurisdiccional y la supervisión independiente. El artículo contempla también la posibilidad de que la Comisión evalúe el nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país. Establece también que, en el ámbito de aplicación de la presente Directiva, será aplicable una decisión general de adecuación adoptada con arreglo a los procedimientos establecidos en el artículo 38 del Reglamento general de protección de datos. Alternativamente, la Comisión puede adoptar una decisión de adecuación exclusivamente a los fines de la presente Directiva.

El artículo 35 define las garantías apropiadas que se necesitan antes de efectuar transferencias internacionales, en ausencia de una decisión de adecuación de la Comisión. Estas garantías pueden ser invocadas mediante un instrumento jurídicamente vinculante, como un acuerdo internacional. Alternativamente, el responsable del tratamiento puede, sobre la base de una evaluación de las circunstancias que concurran en la transferencia, concluir que existen.

El artículo 36 especifica las excepciones para la transferencia de datos, inspirándose en el artículo 26 de la Directiva 95/46/CE y el artículo 13 de la Decisión Marco 2008/977/JAI.

El artículo 37 obliga a los Estados miembros a disponer que el responsable del tratamiento informe al destinatario de toda restricción al tratamiento y tome todas las medidas razonables para garantizar que los destinatarios de los datos personales en el tercer país u organización internacional cumplen estas restricciones.

El artículo 38 establece explícitamente mecanismos de cooperación internacional para la protección de los datos personales entre la Comisión y las autoridades de control de terceros países, en particular aquellos que se considere que ofrecen un nivel de protección adecuado, teniendo en cuenta la Recomendación de la OCDE relativa a la cooperación transfronteriza en la aplicación de las legislaciones que protegen la privacidad, de 12 de junio de 2007.

CAPÍTULO VI – AUTORIDADES NACIONALES DE CONTROL

3.4.5.1. SECCIÓN 1 - INDEPENDENCIA

Sobre la base del artículo 28, apartado 1, de la Directiva 95/46/CE y el artículo 25 de la Decisión Marco 2008/977/JAI, que amplía la misión de las autoridades de control para que contribuyan a la aplicación coherente de la Directiva en toda la Unión, el artículo 39 obliga a los Estados miembros a crear autoridades de control, que pueden ser la creada en virtud del Reglamento general de protección de datos.

El artículo 40, que aplica la jurisprudencia del Tribunal de Justicia de la UE[29], aclara las condiciones para la independencia de las autoridades de control, inspirado también en el artículo 44 del Reglamento (CE) nº 45/2001[30].

El artículo 41 establece las condiciones generales aplicables a los miembros de la autoridad de control, en aplicación de la jurisprudencia pertinente[31] e inspirado también en el artículo 42, apartados 2 a 6, del Reglamento (CE) nº 45/2001.

El artículo 42 establece las normas relativas a la creación de la autoridad de control, incluidas las condiciones de sus miembros, que han de establecer los Estados miembros por ley.

El artículo 43, relativo al secreto profesional de los miembros y el personal de la autoridad de control, sigue lo dispuesto en el artículo 28, apartado 7, de la Directiva 95/46/CE y el artículo 25, apartado 4, de la Decisión Marco 2008/977/JAI.

3.4.5.2. SECCIÓN 2 - FUNCIONES Y PODERES

El artículo 44 establece la competencia de las autoridades de control, sobre la base del artículo 28, apartado 6, de la Directiva 95/46/CE y el artículo 25, apartado 1, DE la Decisión Marco 2008/977/JAI. Cuando ejercen su función jurisdiccional, los órganos jurisdiccionales están exentos de la supervisión por parte de la autoridad de control, aunque no de la aplicación de las normas sustantivas en materia de protección de datos.

El artículo 45 establece la obligación de los Estados miembros de disponer las funciones de la autoridad de control, especialmente la admisión a trámite y la investigación de las reclamaciones y el fomento de la sensibilización de la opinión pública sobre riesgos, normas, garantías y derechos. Cuando se deniegue o restrinja el acceso directo, una función propia de las autoridades de control en el contexto de la presente Directiva es el ejercicio del derecho de acceso por cuenta de los interesados y de verificación de la licitud del tratamiento de datos.

El artículo 46 establece los poderes de la autoridad de control, basándose en el artículo 28, apartado 3, de la Directiva 95/46/CE y el artículo 25, apartados 2 y 3, de la Decisión Marco 2008/977/JAI. Inspirado en el artículo 28, apartado 5, de la Directiva 95/46/CE, el artículo 47 obliga a las autoridades de control a elaborar informes anuales de actividad.

---

29 Tribunal de Justicia de la Unión Europea, sentencia de 9.3.2010, Comisión/Alemania (C-518/07, Rec. 2010, p. I-1885)

30 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; DO L 8 de 12.1.2001, p.1.

31 Op. cit, nota a pie de página nº 27.

3.4.6. CAPÍTULO VII - COOPERACIÓN Y COHERENCIA

El artículo 48 introduce normas sobre la asistencia mutua obligatoria, mientras que el artículo 28, apartado 6, punto 2, de la Directiva 95/46/CE simplemente establecía una obligación general de cooperar, sin especificar más.

El artículo 49 establece que el Consejo Europeo de Protección de Datos, establecido por el Reglamento general de protección de datos, también ejerce sus funciones en relación con las actividades de tratamiento en el ámbito de aplicación de la presente Directiva. Con el fin de proporcionar apoyo complementario, la Comisión solicitará el asesoramiento de representantes de las autoridades de los Estados miembros competentes para la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, así como de representantes de Europol y Eurojust, por medio de un grupo de expertos en los aspectos relacionados con la función coercitiva de la protección de datos.

3.4.7. CAPÍTULO VIII – RECURSOS, RESPONSABILIDAD Y SANCIONES

Inspirado en el artículo 28, apartado 4, de la Directiva 95/46/CE, el artículo 50 establece el derecho de todo interesado a presentar una reclamación ante una autoridad de control, y se refiere a cualquier infracción de la Directiva en relación con el reclamante. Asimismo especifica los organismos, organizaciones o asociaciones que pueden presentar una reclamación en nombre del interesado y también en caso de violación de datos personales, con independencia de la reclamación de un interesado.

El artículo 51 se refiere al derecho a un recurso judicial contra una autoridad de control. Se basa en la disposición general del artículo 28, apartado 3, de la Directiva 95/46/CE y establece expresamente que el interesado puede ejercitar acciones judiciales para obligar a la autoridad de control a actuar a raíz de una reclamación.

Basado en el artículo 22 de la Directiva 95/46/CE y en el artículo 20 de la Decisión Marco 2008/977/JAI, el artículo 52 se refiere al derecho a un recurso judicial contra un responsable o encargado del tratamiento.

El artículo 53 introduce normas comunes aplicables a los procedimientos judiciales, incluidos los derechos de los organismos, organizaciones o asociaciones de representar a los interesados ante los órganos jurisdiccionales, y el derecho de las autoridades de control a ejercitar acciones jurisdiccionales. La obligación de los Estados miembros de garantizar la celeridad de las acciones se inspira en el artículo 18, apartado 1, de la Directiva 2000/31/CE sobre comercio electrónico[32].

El artículo 54 obliga a los Estados miembros a establecer el derecho de indemnización. Inspirado en el artículo 23 de la Directiva 95/46/CE y en el artículo 19, apartado 1, de la Decisión Marco 2008/977/JAI, amplía este derecho a los perjuicios causados por los encargados del tratamiento y aclara la responsabilidad de los corresponsables y coencargados.

---

[32] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior («Directiva sobre el comercio electrónico»); DO L 178 de 17.07.2000, p. 1.

El artículo 55 obliga a los Estados miembros a establecer normas relativas a las sanciones, a sancionar las infracciones de la Directiva, y a garantizar su aplicación.

3.4.8. CAPÍTULO IX – ACTOS DELEGADOS Y ACTOS DE EJECUCIÓN

El artículo 56 contiene disposiciones normalizadas para el ejercicio de las delegaciones en consonancia con el artículo 290 del TFUE. Ello permite al legislador delegar en la Comisión los poderes para adoptar actos no legislativos de alcance general que completen o modifiquen determinados elementos no esenciales de un acto legislativo (actos cuasi legislativos).

El artículo 57 contiene la disposición relativa al procedimiento del comité necesario para la atribución de competencias de ejecución a la Comisión en los casos en que, de conformidad con el artículo 291 del TFUE, se requieran condiciones uniformes de ejecución de los actos jurídicamente vinculantes de la Unión. Es de aplicación el procedimiento de examen.

3.4.9. CAPÍTULO X - DISPOSICIONES FINALES

El artículo 58 deroga la Decisión Marco 2008/977/JAI.

El artículo 59 establece que se mantienen inalteradas las disposiciones específicas en lo que respecta al tratamiento de datos personales por parte de autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales en actos de la Unión adoptados antes de la fecha de adopción de la presente Directiva que regulen el tratamiento de datos personales o el acceso a los sistemas de información establecidos en el ámbito de aplicación de la misma.

El artículo 60 aclara la relación de la presente Directiva con los acuerdos internacionales celebrados anteriormente por los Estados miembros en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.

El artículo 61 establece la obligación de la Comisión de evaluar e informar sobre la aplicación de la Directiva, a fin de determinar la necesidad de adaptar a la presente Directiva las disposiciones específicas adoptadas anteriormente contempladas en el artículo 59.

El artículo 62 establece la obligación de los Estados miembros de incorporar la Directiva a sus legislaciones nacionales y de comunicar a la Comisión las disposiciones adoptadas de conformidad con la misma.

El artículo 63 determina la fecha de la entrada en vigor de la Directiva.

El artículo 64 establece los destinatarios de la Directiva.

4. IMPLICACIONES PRESUPUESTARIAS

La ficha financiera legislativa que acompaña a la propuesta de Reglamento general de protección de datos comprende la incidencia presupuestaria del Reglamento y de la presente Directiva.

2012/0010 (COD)

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 16, apartado 2,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Previa consulta del Supervisor Europeo de Protección de Datos[33],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea establecen que toda persona tiene derecho a la protección de los datos personales que le conciernan.

(2) El tratamiento de datos personales está al servicio del hombre; los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea la nacionalidad o residencia de estas personas, respetar las libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. Debe contribuir a la plena realización de un espacio de libertad, seguridad y justicia.

(3) La rápida evolución tecnológica y la globalización han supuesto nuevos retos para la protección de los datos personales. Se ha incrementado de manera espectacular la magnitud del intercambio y la recogida de datos. La tecnología permite que las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades.

[33] DO C de …, p. ...

(4) Ello requiere facilitar la libre circulación de datos entre las autoridades competentes en el seno de la Unión y la transferencia a terceros países y organizaciones internacionales, al tiempo que se garantiza un alto nivel de protección de los datos personales. Exige el establecimiento de un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta.

(5) 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[34], se aplica a todas las actividades de tratamiento de datos personales en los Estados miembros tanto en el sector público como en el privado. Sin embargo, no se aplica al tratamiento de datos personales efectuado «en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario», como las actividades en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.

(6) La Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal[35], es aplicable en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial. El ámbito de aplicación de esta Decisión Marco se limita al tratamiento de los datos personales transmitidos o puestos a disposición entre los Estados miembros.

(7) Asegurar un nivel uniforme y elevado de protección de los datos personales de las personas físicas y facilitar el intercambio de datos personales entre las autoridades competentes de los Estados miembros es esencial para garantizar la eficacia de la cooperación judicial en materia penal y de la cooperación policial. A tal efecto, el nivel de protección de los derechos y libertades de las personas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, debe ser equivalente en todos los Estados miembros. La protección efectiva de los datos personales en la Unión no solo requiere la consolidación de los derechos de los interesados y de las obligaciones de quienes tratan dichos datos personales, sino también poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos personales en los Estados miembros.

(8) El artículo 16, apartado 2, del Tratado de Funcionamiento de la Unión Europea dispone que el Parlamento Europeo y el Consejo deben establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal y las normas relativas a la libre circulación de estos datos.

(9) Sobre esta base, el Reglamento UE …../2012 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), establece las normas generales para proteger a las personas físicas en relación con el tratamiento de los datos personales y para garantizar la libre circulación de los datos personales en la Unión.

---

34 DO L 281 de 23.11.1995, p. 31.

35 DO L 350 de 30.12.2008, p. 60.

(10) En la Declaración 21 relativa a la protección de los datos de carácter personal en el ámbito de la cooperación judicial en materia penal y la cooperación policial, aneja al Acta final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa, la Conferencia reconoció que podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, en razón de la naturaleza específica de dichos ámbitos.

(11) Por lo tanto, una nueva Directiva debe responder a la naturaleza específica de estos ámbitos y establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

(12) A fin de garantizar el mismo nivel de protección de las personas a través de derechos exigibles legalmente en toda la Unión y evitar divergencias que dificulten el intercambio de datos personales entre las autoridades competentes, la Directiva debe establecer normas armonizadas para la protección y la libre circulación de los datos personales en los ámbitos de la cooperación judicial en materia penal y la cooperación policial.

(13) La presente Directiva permite que se tenga en cuenta el principio de acceso público a los documentos oficiales al aplicar las disposiciones de la misma.

(14) La protección otorgada por la presente Directiva atañe a las personas físicas, independientemente de su nacionalidad o lugar de residencia, en relación con el tratamiento de datos personales.

(15) La protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas, pues de lo contrario daría lugar a graves riesgos de elusión. La protección de las personas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, si los datos están contenidos o destinados a ser incluidos en un fichero. Los ficheros o conjuntos de ficheros y sus carpetas que no estén estructurados con arreglo a criterios específicos no están comprendidos en el ámbito de aplicación de la presente Directiva. La presente Directiva no debe aplicarse al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión, en particular en lo que respecta a la seguridad nacional, o a los datos tratados por instituciones, órganos y organismos de la Unión, tales como Europol o Eurojust.

(16) Los principios de protección deben aplicarse a toda información relativa a una persona identificada o identificable. Para determinar si una persona física es identificable deben tenerse en cuenta todos los medios que razonablemente pudiera utilizar el responsable del tratamiento o cualquier otro individuo para identificar a dicha persona. Los principios de protección de datos no deben aplicarse a los datos convertidos en anónimos de forma que el interesado a quien se refieren ya no resulte identificable.

(17) Los datos personales relacionados con la salud deben incluir en particular todos los datos relativos a la salud del interesado; información sobre el registro de la persona para la prestación de servicios sanitarios; información acerca de los pagos o de la

admisibilidad para la atención sanitaria con respecto a la persona; un número, símbolo u otro dato asignado a una persona que la identifica de manera unívoca a efectos de salud; cualquier información acerca de la persona recogida durante la prestación de servicios sanitarios a esta; información derivada de las pruebas o los exámenes de una parte del cuerpo o sustancia corporal, incluidas muestras biológicas; identificación de una persona como prestador de asistencia sanitaria a la persona; o cualquier información sobre, por ejemplo, toda enfermedad, discapacidad, riesgo de enfermedades, historia médica, tratamiento clínico, o estado fisiológico o biomédico real del interesado, independientemente de su fuente, como, por ejemplo, cualquier médico u otro profesional de la sanidad, hospital, dispositivo médico, o prueba diagnóstica in vitro.

(18) Todo tratamiento de datos de carácter personal debe efectuarse de forma lícita, justa y transparente en relación con las personas afectadas. En particular, los fines específicos para los que se hayan tratado los datos deben ser explícitos.

(19) Para la prevención, investigación y enjuiciamiento de infracciones penales, es necesario que las autoridades competentes conserven y traten datos personales, recogidos en el contexto de la prevención, investigación, detección o enjuiciamiento de infracciones penales, más allá de ese contexto específico, con el fin de adquirir un mejor conocimiento de las tendencias y fenómenos delictivos, recabar información sobre las redes de delincuencia organizada, y establecer vínculos entre las distintas infracciones detectadas.

(20) Los datos personales no deben ser tratados para fines incompatibles con la finalidad para la que fueron recogidos. Los datos deben ser adecuados, pertinentes y no excesivos para los fines para los que se traten. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos.

(21) El principio de exactitud de los datos debe aplicarse teniendo presente el carácter y finalidad del tratamiento correspondiente. En particular en los procedimientos judiciales, las declaraciones que contienen datos personales se basan en la percepción subjetiva de las personas y, en algunos casos, no siempre son verificables. En consecuencia, el requisito de exactitud no debe relacionarse con la exactitud de una afirmación, sino exclusivamente con el hecho de que se ha formulado una afirmación concreta.

(22) En la interpretación y aplicación de los principios generales relativos al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, se han de tener en cuenta las características específicas del sector, incluidos los objetivos específicos perseguidos.

(23) Es inherente al tratamiento de datos personales en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se traten datos personales relativos a diferentes categorías de interesados. Por tanto, en la medida de lo posible, se debe distinguir claramente entre los datos personales de diferentes categorías de interesados tales como los sospechosos, los condenados por una infracción penal, las víctimas y terceros, como los testigos, las personas que posean información o contactos útiles y los cómplices de sospechosos y delincuentes condenados.

(24) En la medida de lo posible, debe distinguirse entre los datos personales en función de su grado de exactitud y fiabilidad. Se debe distinguir entre hechos y apreciaciones personales, con el fin de garantizar tanto la protección de las personas como la calidad y fiabilidad de la información tratada por las autoridades competentes.

(25) Para que sea lícito, el tratamiento de datos personales debe ser necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, para el cumplimiento de una misión de interés público por una autoridad competente prevista por ley, o con el fin de proteger los intereses vitales del interesado o de otra persona, o bien para la prevención de una amenaza inminente y grave para la seguridad pública.

(26) Protección específica merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos fundamentales o la intimidad, incluidos los datos genéticos. Tales datos no deben ser tratados, a no ser que el tratamiento esté específicamente autorizado por una ley que contemple medidas adecuadas para proteger los intereses legítimos del interesado, sea necesario para salvaguardar el interés vital del interesado o de otra persona; o se refiera a datos que el interesado ha hecho manifiestamente públicos.

(27) Toda persona física debe tener derecho a no ser objeto de una medida que se base únicamente en el tratamiento automático si produce un efecto jurídico desfavorable para él, salvo que esté autorizada por ley y sujeta a medidas adecuadas para salvaguardar los intereses legítimos del interesado.

(28) Para poder ejercer sus derechos, cualquier información que se facilite al interesado debe ser fácilmente accesible y fácil de entender, utilizando un lenguaje sencillo y claro.

(29) Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos establecidos en la presente Directiva, incluidos los mecanismos para solicitar de forma gratuita, entre otras cosas, el acceso a los datos, su rectificación y supresión. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin demora injustificada.

(30) El principio de tratamiento leal exige que el interesado sea informado, entre otras cosas, de la existencia de la operación de tratamiento y sus fines, del plazo de conservación de los datos, de la existencia del derecho de acceso, rectificación o supresión y del derecho a presentar una reclamación. Cuando los datos se obtengan de los interesados, estos también deben ser informados de si están obligados a facilitarlos y de las consecuencias, en caso de que no lo hicieran.

(31) La información sobre el tratamiento de los datos de carácter personal relativos a los interesados debe ser facilitada a estos últimos en el momento de su recogida, o, si los datos no se recogieran de los interesados, en el momento del registro o en un plazo razonable después de la recogida, habida cuenta de las circunstancias específicas en que se traten los datos.

(32) Toda persona debe tener el derecho de acceder a los datos recogidos que le conciernan y a ejercer este derecho con facilidad, con el fin de conocer y verificar la licitud del tratamiento. Todo interesado debe, por tanto, tener el derecho de conocer y de que se

le comuniquen, en particular, los fines para los que se tratan los datos, el plazo de su conservación, los destinatarios que los reciben, incluso en terceros países. Se debe autorizar a los interesados a recibir una copia de sus datos personales que estén siendo tratados.

(33) Debe permitirse a los Estados miembros adoptar medidas legislativas que retrasen, restrinjan u omitan la información de los interesados o el acceso a sus datos personales en la medida y siempre que dicha restricción total o parcial constituya una medida necesaria y proporcionada en una sociedad democrática, teniendo debidamente en cuenta los intereses legítimos de la persona de que se trate, con el fin de no entorpecer las indagaciones, investigaciones o procedimientos oficiales o jurídicos, de no perjudicar la prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, de proteger la seguridad pública o la seguridad nacional o de proteger al interesado o los derechos y libertades de otras personas.

(34) Toda denegación o restricción de acceso debe comunicarse por escrito al interesado, incluidas las razones de hecho o de Derecho sobre las que se basa la decisión.

(35) Cuando los Estados miembros hayan adoptado medidas legislativas que restrinjan, total o parcialmente, el derecho de acceso, el interesado debe tener derecho a solicitar que la autoridad nacional de control competente verifique la licitud del tratamiento. El interesado debe ser informado de este derecho. Cuando el acceso sea ejercido por la autoridad de control por cuenta del interesado, este debe ser informado por la autoridad de control, como mínimo, de que se han llevado a cabo las verificaciones necesarias y del resultado en cuanto a la licitud del tratamiento en cuestión.

(36) Toda persona debe tener derecho a que se rectifiquen los datos personales inexactos que le conciernan y a que se supriman, cuando el tratamiento de estos datos no cumpla los principios esenciales establecidos en la presente Directiva. Cuando los datos personales se sometan a tratamiento en el transcurso de investigaciones y procedimientos penales, los derechos de información, acceso, rectificación, supresión y restricción del tratamiento pueden ejercerse de conformidad con las normas nacionales relativas a los procedimientos judiciales.

(37) Se debe establecer la responsabilidad general del responsable por cualquier tratamiento de datos personales realizado por él mismo o en su nombre. En particular, el responsable del tratamiento debe garantizar que las operaciones de tratamiento se ajustan a las normas adoptadas con arreglo a la presente Directiva.

(38) La protección de los derechos y libertades de los interesados con respecto al tratamiento de datos personales exige la adopción de las oportunas medidas de carácter técnico y organizativo con el fin de garantizar el cumplimiento de lo dispuesto en la presente Directiva. Con objeto de velar por el cumplimiento de las disposiciones adoptadas con arreglo a la presente Directiva, el responsable debe adoptar las políticas y aplicar las medidas adecuadas que cumplan especialmente los principios de protección de datos desde el diseño y por defecto.

(39) La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, requieren una atribución clara de las responsabilidades con arreglo a la presente Directiva, incluidos

los casos en que un responsable determine los fines, condiciones y medios del tratamiento de forma conjunta con otros responsables del tratamiento o cuando el tratamiento se efectúe por cuenta de un responsable.

(40) Con objeto de supervisar el cumplimiento de lo dispuesto en la presente Directiva, el responsable o el encargado del tratamiento deben documentar las actividades de tratamiento. Los responsables y encargados del tratamiento deben estar obligados a cooperar con la autoridad de control y a difundir esta documentación, previa solicitud, de modo que pueda servir para supervisar las operaciones de tratamiento.

(41) Con el fin de garantizar la protección efectiva de los derechos y libertades de los interesados mediante acciones preventivas, el responsable o encargado del tratamiento deben consultar, en determinados casos, a la autoridad de control antes del tratamiento.

(42) Si no se toman medidas de manera rápida y adecuada, las violaciones de los datos personales pueden entrañar un perjuicio, incluso para la reputación de la persona en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación, debe notificarla a la autoridad nacional competente. Las personas físicas cuyos datos personales o intimidad puedan verse afectados negativamente por dicha violación deben ser informadas de ello sin demora injustificada para que puedan adoptar las cautelas necesarias. Se debe considerar que una violación afecta negativamente a los datos personales o la intimidad de los interesados cuando conlleva, por ejemplo, fraude o usurpación de identidad, daños físicos, humillación grave o perjuicio para su reputación en relación con el tratamiento de datos personales.

(43) Al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de datos personales, conviene tener debidamente en cuenta las circunstancias de la violación, incluyendo si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas, limitando eficazmente la probabilidad de uso indebido. Asimismo, estas normas y procedimientos deben tener en cuenta los intereses legítimos de las autoridades competentes, en los casos en que una comunicación temprana pudiera obstaculizar innecesariamente la investigación de las circunstancias de la violación.

(44) El responsable o el encargado del tratamiento deben designar a una persona que les ayude a supervisar el cumplimiento de las disposiciones adoptadas con arreglo a la presente Directiva. Varias entidades de la autoridad competente pueden designar conjuntamente a un delegado de protección de datos. Los delegados de protección de datos deben estar en condiciones de desempeñar sus funciones y tareas con independencia y eficacia.

(45) Los Estados miembros deben velar por que una transferencia a un tercer país solo se lleve a cabo si es necesaria para la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y si el responsable del tratamiento en el tercer país u organización internacional es una autoridad competente a tenor de la presente Directiva. Puede llevarse a cabo una transferencia en los casos en que la Comisión haya decidido que el tercer país o la organización internacional de que se trate garantizan un nivel adecuado de protección, o cuando se hayan ofrecido unas garantías apropiadas.

(46) La Comisión puede determinar, con efectos para toda la Unión, que algunos terceros países, un territorio o un sector del tratamiento en un tercer país, o una organización internacional ofrecen un nivel adecuado de protección de datos, proporcionando así seguridad jurídica y uniformidad en toda la Unión en lo que se refiere a los terceros países u organizaciones internacionales que se considera aportan tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin tener que obtener ninguna otra autorización.

(47) En consonancia con los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos, la Comisión debe tener en cuenta en qué medida en dicho tercer país se respeta el Estado de Derecho, el acceso a la justicia, así como las normas y principios internacionales relativos a los derechos humanos.

(48) La Comisión también debe poder reconocer que un tercer país, un territorio, un sector del tratamiento en un tercer país, o una organización internacional no ofrece un nivel adecuado de protección de datos. En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país, salvo cuando se base en un acuerdo internacional, unas garantías apropiadas o una excepción. Deben establecerse los procedimientos para celebrar consultas entre la Comisión y dichos terceros países u organizaciones internacionales. Sin embargo, tal decisión de la Comisión se entenderá sin perjuicio de la posibilidad de llevar a cabo transferencias sobre la base de garantías apropiadas o de una excepción establecida en la Directiva.

(49) Las transferencias no basadas en dicha decisión de adecuación solo deben permitirse cuando se hayan invocado las garantías apropiadas en un instrumento jurídicamente vinculante que garantice la protección de los datos personales o cuando el responsable o encargado del tratamiento haya evaluado todas las circunstancias que rodean la operación de transferencia de datos o el conjunto de operaciones de transferencia de datos y, basándose en esta evaluación, considere que existen las garantías apropiadas con respecto a la protección de los datos personales. En los casos en que no existan razones para autorizar una transferencia, deben permitirse excepciones, si fuera necesario, para proteger el interés vital del interesado o de otra persona, o para proteger intereses legítimos del interesado en caso de que la legislación del Estado miembro que transfiere los datos personales así lo disponga, o cuando sea indispensable para prevenir una amenaza inminente y grave para la seguridad pública de un Estado miembro o de un tercer país, o en determinados casos a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, o en casos específicos para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

(50) Cuando los datos personales circulan a través de las fronteras se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer los derechos de protección de datos con el fin de protegerse contra la utilización ilícita o la revelación de dichos datos. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. Sus esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por poderes preventivos o correctores insuficientes y regímenes jurídicos incoherentes. Por tanto, es necesario fomentar una cooperación más estrecha entre las autoridades de control de la protección de datos para ayudarles a intercambiar información con sus homólogos extranjeros.

(51) La creación en los Estados miembros de autoridades de control que ejerzan sus funciones con plena independencia constituye un elemento esencial de la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal. Las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas en aplicación de la presente Directiva y contribuir a su aplicación coherente en toda la Unión, con el fin de proteger a las personas físicas en relación con el tratamiento de sus datos de carácter personal. Para ello, las autoridades de supervisión deben cooperar entre sí y con la Comisión.

(52) Los Estados miembros pueden confiar a una autoridad de control ya creada en los Estados miembros de conformidad con el Reglamento (UE) nº …./2012 la responsabilidad de las funciones que corresponden a las autoridades nacionales de control que han de crearse con arreglo a lo dispuesto en la presente Directiva.

(53) Se debe autorizar a los Estados miembros a crear más de una autoridad de control con objeto de reflejar su estructura constitucional, organizativa y administrativa. Todas las autoridades de control deben estar dotadas de los recursos financieros y humanos adecuados, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus tareas, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión.

(54) Las condiciones generales aplicables a los miembros de la autoridad de control deben establecerse por ley en cada Estado miembro, y disponer, entre otras cosas, que dichos miembros deben ser nombrados por el Parlamento o el Gobierno del Estado miembro, e incluir normas sobre su cualificación personal y función.

(55) Aunque la presente Directiva también se aplica a las actividades de los órganos jurisdiccionales nacionales, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los primeros actúen en ejercicio de su función jurisdiccional, con el fin de garantizar la independencia de los jueces en el desempeño de sus funciones. No obstante, esta excepción debe limitarse estrictamente a verdaderas actividades judiciales en juicios y no debe aplicarse a otras actividades en las que puedan estar implicados los jueces, de conformidad con el Derecho nacional.

(56) Para garantizar la supervisión y ejecución coherentes de la presente Directiva en toda la Unión, las autoridades de control deben gozar en todos los Estados miembros de las mismas funciones y poderes efectivos, incluidos los poderes de investigación, de intervención jurídicamente vinculante, de decisión y sanción, especialmente en casos de reclamaciones de personas físicas, y la capacidad de litigar.

(57) Cada autoridad de control debe oír las reclamaciones presentadas por cualquier interesado y debe investigar el asunto. La investigación a raíz de una reclamación debe llevarse a cabo, bajo control jurisdiccional, en la medida en que sea adecuada en el caso específico. La autoridad de control debe informar al interesado de la evolución y el resultado de la reclamación en un plazo razonable. Si el caso requiere una mayor investigación o coordinación con otra autoridad de control, se debe facilitar información intermedia al interesado.

(58) Las autoridades de control deben ayudarse en el desempeño de sus funciones y facilitarse ayuda mutua, con el fin de garantizar la aplicación y ejecución coherentes de las disposiciones adoptadas con arreglo a la presente Directiva.

(59) El Consejo Europeo de Protección de Datos creado por el Reglamento (UE) nº …./2012 debe contribuir a la aplicación coherente de la presente Directiva en el conjunto de la Unión, entre otras cosas, asesorando a la Comisión y fomentando la cooperación de las autoridades de control en toda la Unión.

(60) Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control en cualquier Estado miembro y a presentar un recurso judicial si considera que se vulneran sus derechos en el marco de la presente Directiva o en caso de que la autoridad de control no reaccione ante una reclamación o no actúe cuando dicha medida sea necesaria para proteger los derechos del interesado.

(61) Toda entidad, organización o asociación que tenga por objeto proteger los derechos e intereses de los interesados en relación con la protección de sus datos y esté constituida con arreglo a la legislación de un Estado miembro debe tener derecho a presentar una reclamación ante la autoridad de control o ejercer el derecho de recurso judicial, en nombre de los interesados, o a presentar, independientemente de la reclamación de un interesado, su propia reclamación, cuando considere que se ha producido una violación de los datos personales.

(62) Toda persona física o jurídica debe tener derecho a presentar un recurso judicial contra las decisiones de una autoridad de control que le conciernan. Las acciones legales contra una autoridad de control deben ejercitarse ante los órganos jurisdiccionales del Estado miembro en el que esté establecida la autoridad de control.

(63) Los Estados miembros deben garantizar que las acciones judiciales, para ser eficaces, permitan la rápida adopción de medidas con el fin de corregir o impedir una infracción a la presente Directiva.

(64) Cualquier perjuicio que pueda sufrir una persona como consecuencia de un tratamiento ilícito debe ser compensado por el responsable o el encargado del tratamiento, que pueden quedar exentos de responsabilidad si demuestran que no son responsables del perjuicio, en particular si acreditan la conducta culposa del interesado o en caso de fuerza mayor.

(65) Deben imponerse sanciones a toda persona física o jurídica, ya sean de Derecho público o privado, que no cumpla lo dispuesto en la presente Directiva. Los Estados miembros deben asegurarse de que las sanciones sean efectivas, proporcionadas y disuasorias y deben tomar todas las medidas para su aplicación.

(66) Con el fin de cumplir los objetivos de la presente Directiva, a saber, proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales y garantizar el libre intercambio de datos personales por parte de las autoridades competentes en la Unión, debe delegarse a la Comisión la facultad de adoptar actos de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea. En particular, los actos delegados deben adoptarse con respecto de las notificaciones de una violación de datos personales a la autoridad de control. Es de especial importancia que la Comisión evacue las consultas apropiadas durante sus trabajos preparatorios, con expertos inclusive. La Comisión, al preparar y elaborar actos delegados, debe garantizar una transmisión simultánea, oportuna y apropiada de los documentos pertinentes al Parlamento Europeo y al Consejo.

(67) Con el fin de garantizar unas condiciones uniformes para la aplicación de la presente Directiva, se deben conferir competencias de ejecución a la Comisión por lo que respecta a la documentación por parte de los responsables y encargados del tratamiento; la seguridad del tratamiento, especialmente en lo que se refiere a las normas de cifrado; la notificación de una violación de los datos personales a la autoridad de control, y el nivel adecuado de protección que ofrece un tercer país, un territorio, un sector de tratamiento en dicho tercer país o una organización internacional. Estas competencias deben ejercerse de conformidad con el Reglamento (UE) nº 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión[36].

(68) El procedimiento de examen debe emplearse para la adopción de medidas por lo que respecta a la documentación por parte de los responsables y encargados del tratamiento; la seguridad del tratamiento, especialmente en lo que se refiere a las normas de cifrado; la notificación de una violación de los datos personales a la autoridad de control; y el nivel adecuado de protección que ofrece un tercer país, un territorio, un sector de tratamiento en dicho tercer país o una organización internacional, dado que dichos actos son de alcance general.

(69) La Comisión debe adoptar actos de ejecución inmediatamente aplicables cuando así lo requieran razones perentorias, en casos debidamente justificados relacionados con un tercer país, un territorio o un sector de tratamiento en ese tercer país, o una organización internacional que no garantice un nivel de protección adecuado.

(70) Dado que los objetivos de la presente Directiva, a saber, proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales y garantizar el libre intercambio de datos personales por parte de las autoridades competentes en la Unión, no pueden ser alcanzados de manera suficiente por los Estados miembros y, por consiguiente, debido a la escala o los efectos de la actuación, pueden lograrse mejor a nivel de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar dicho objetivo.

(71) La Decisión Marco 2008/977/JAI debe ser derogada por la presente Directiva.

(72) No deben verse afectadas las disposiciones específicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales en los actos de la Unión que hayan sido adoptados antes de la fecha de adopción de la presente Directiva, que regulan el tratamiento de los datos personales entre los Estados miembros o el acceso de las autoridades designadas de los Estados miembros a los sistemas de información establecidos con arreglo a lo dispuesto en los Tratados. La Comisión debe evaluar la situación con respecto a la relación entre la presente Directiva y los actos adoptados con anterioridad

[36] DO L 55 de 28.2.2011, p. 13.

a su fecha de adopción que regulan el tratamiento de los datos personales entre los Estados miembros o el acceso de las autoridades designadas de los Estados miembros a los sistemas de información establecidos con arreglo a lo dispuesto en los Tratados, a fin de evaluar la necesidad de ajustar estas disposiciones específicas a la presente Directiva.

(73) Con el fin de garantizar una protección amplia y coherente de los datos personales en la Unión, los acuerdos internacionales celebrados por los Estados miembros con anterioridad a la entrada en vigor de la presente Directiva deben modificarse en consonancia con lo dispuesto en la misma.

(74) La presente Directiva se entiende sin perjuicio de las normas relativas a la lucha contra los abusos sexuales, la explotación sexual de los niños, y la pornografía infantil, tal como se establecen en la Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011[37].

(75) De conformidad con el artículo 6*bis* del Protocolo sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, las normas establecidas en la presente Directiva solo serán vinculantes para el Reino Unido o Irlanda en la medida en que sean vinculantes para estos Estados normas de la Unión que regulen formas de cooperación judicial en materia penal y de cooperación policial en cuyo marco deban respetarse las disposiciones establecidas basándose en el artículo 16 del Tratado de Funcionamiento de la Unión Europea.

(76) De conformidad con lo dispuesto en los artículos 2 y 2*bis* del Protocolo sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no queda obligada por la presente Directiva ni está sujeta a su aplicación. Dado que la presente Directiva desarrolla el acervo de Schengen en el marco de las disposiciones del título V de la parte tres del Tratado de Funcionamiento de la Unión Europea, de conformidad con el artículo 4 del Protocolo, Dinamarca debe decidir, en un plazo de seis meses a partir de la adopción de la presente Directiva, si lo incorpora a su legislación nacional.

(77) Por lo que se refiere a Islandia y Noruega, la presente Directiva constituye un desarrollo de las disposiciones del acervo de Schengen, como se establece en el Acuerdo celebrado por el Consejo de la Unión Europea con la República de Islandia y el Reino de Noruega sobre la asociación de estos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen[38].

(78) Por lo que respecta a Suiza, la presente Directiva constituye un desarrollo de las disposiciones del acervo de Schengen, como se establece en el Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen[39].

(79) Por lo que respecta a Liechtenstein, la presente Directiva constituye un desarrollo de las disposiciones del acervo de Schengen, como se establece en el Protocolo entre la

---

37 DO L 335 de 17.12.2011, p. 1.
38 DO L 176 de 10.7.1999, p. 36.
39 DO L 53 de 27.2.2008, p. 52.

Unión Europea, la Comunidad Europea, la Confederación Suiza y el Principado de Liechtenstein sobre la adhesión del Principado de Liechtenstein al Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen[40].

(80) La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea, consagrados en el Tratado, en particular el derecho al respeto de la vida privada y familiar, el derecho a la protección de los datos personales, el derecho a la tutela judicial efectiva y a un juicio justo. Las limitaciones aplicadas a estos derechos son conformes al artículo 52, apartado 1, de la Carta ya que son necesarias para alcanzar objetivos de interés general reconocidos por la Unión o la necesidad de protección de los derechos y libertades de otras personas.

(81) De conformidad con la Declaración política conjunta de los Estados miembros y de la Comisión sobre los documentos explicativos de 28 de septiembre de 2011, los Estados miembros se han comprometido a adjuntar a la notificación de sus medidas de transposición, cuando esté justificado, uno o varios documentos que expliquen la relación entre los elementos de una directiva y las partes correspondientes de los instrumentos nacionales de transposición. Con respecto a la presente Directiva, el legislador considera que la transmisión de estos documentos está justificada.

(82) La presente Directiva no impedirá que los Estados miembros regulen el ejercicio de los derechos de los interesados sobre información, acceso, rectificación, supresión y restricción de sus datos personales tratados en el marco de un procedimiento penal, y sus posibles restricciones, en las normas nacionales en materia de enjuiciamiento penal.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1
Objeto y objetivos

1. La presente Directiva establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

2. De conformidad con la presente Directiva, los Estados miembros deberán:

   a) proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales; y

[40] DO L 160 de 18.6.2011, p. 19.

b) garantizar que el intercambio de datos personales por parte de las autoridades competentes en el interior de la Unión no quede restringido ni prohibido por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Artículo 2
Ámbito de aplicación

1. La presente Directiva se aplica al tratamiento de datos personales por parte de las autoridades competentes a los fines mencionados en el artículo 1, apartado 1.

2. La presente Directiva se aplicará al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

3. La presente Directiva no se aplicará al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión, en particular en lo que respecta a la seguridad nacional;

b) por parte de las instituciones, órganos u organismos de la Unión.

Artículo 3
Definiciones

A efectos de la presente Directiva se entenderá por:

1) «interesado»: toda persona física identificada o que pueda ser identificada, directa o indirectamente, por medios que puedan ser utilizados razonablemente por el responsable del tratamiento o por cualquier otra persona física o jurídica, en particular mediante un número de identificación, datos de localización, identificador en línea o uno o varios elementos específicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «datos personales»: toda información relativa a un interesado;

3) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, efectuadas o no mediante procedimientos automatizados, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, supresión o destrucción;

4) «restricción de tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

5) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

6) «responsable del tratamiento»: la autoridad pública competente que sola o conjuntamente con otras determine los fines, condiciones y medios del tratamiento de datos personales; en caso de que los fines, condiciones y medios del tratamiento estén determinados por el Derecho de la Unión o la legislación de los Estados miembros, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho de la Unión o por la legislación de los Estados miembros;

7) «encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;

8) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos personales;

9) «violación de datos personales»: toda violación de la seguridad que ocasione la destrucción accidental o ilícita, la pérdida, alteración, comunicación no autorizada o el acceso a datos personales transmitidos, conservados o tratados de otra forma;

10) «datos genéticos»: todos los datos, con independencia de su tipo, relativos a las características de una persona que sean hereditarias o adquiridas durante el desarrollo prenatal temprano;

11) «datos biométricos»: cualesquiera datos relativos a las características físicas, fisiológicas o conductuales de una persona que permitan su identificación única, como imágenes faciales o datos dactiloscópicos;

12) «datos relativos a la salud»: cualquier información que se refiera a la salud física o mental de una persona, o a la asistencia prestada por los servicios de salud a la persona;

13) «niño»: toda persona menor de 18 años;

14) «autoridades competentes»: toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales;

15) «autoridad de control»: la autoridad pública establecida por un Estado miembro de acuerdo con el artículo 39.

CAPÍTULO II
PRINCIPIOS

Artículo 4
Principios relativos al tratamiento de datos personales

Los Estados miembros dispondrán que los datos personales deben ser:

a) tratados de manera lícita y leal;

b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines;

c) adecuados, pertinentes y no excesivos en relación con los fines para los que se traten;

d) exactos y, si fuera necesario, mantenerse actualizados; se deben adoptar todas las medidas razonables para que se supriman o rectifiquen sin demora los datos personales que sean inexactos con respecto a los fines para los que se traten;

e) conservados en una forma que permita identificar al interesado durante un periodo no superior al necesario para los fines para los que se someten a tratamiento;

f) tratados bajo la responsabilidad del responsable del tratamiento, que garantizará el cumplimiento de las disposiciones adoptadas con arreglo a la presente Directiva.

.

Artículo 5
Distinción entre diferentes categorías de interesados

1. Los Estados miembros dispondrán que, en la medida de lo posible, el responsable del tratamiento establecerá una distinción clara entre los datos personales de las distintas categorías de interesados, tales como:

a) personas respecto de las cuales existan motivos fundados para presumir que han cometido o van a cometer una infracción penal;

b) personas condenadas por una infracción penal;

c) víctimas de una infracción penal o personas respecto de las cuales existan motivos fundados para presumir que pueden ser víctimas de una infracción penal;

d) terceras partes involucradas en una infracción penal como, por ejemplo, personas que puedan ser citadas para testificar en investigaciones relacionadas con infracciones penales o procedimientos penales ulteriores, o personas que puedan facilitar información sobre infracciones penales, o personas de contacto o asociados de una de las personas mencionadas en las letras a) y b); y

e) personas que no entren dentro de ninguna de las categorías contempladas más arriba.

Artículo 6

Diferentes grados de exactitud y fiabilidad de los datos personales

1. Los Estados miembros velarán por que, en la medida de lo posible, las diferentes categorías de datos personales objeto de tratamiento se distingan según su grado de exactitud y fiabilidad.

2. Los Estados miembros velarán por que, en la medida de lo posible, los datos personales basados en hechos se distingan de los datos personales basados en apreciaciones personales.

Artículo 7

Licitud del tratamiento de datos

Los Estados miembros dispondrán que el tratamiento de datos personales solo será lícito en la medida en que sea necesario:

a) para la ejecución de una tarea realizada por una autoridad competente, basada en la ley, para los fines establecidos en el artículo 1, apartado 1; o

b) para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

c) con el fin de proteger los intereses vitales del interesado o de otra persona; o

d) a fin de prevenir una amenaza inminente y grave para la seguridad pública.

Artículo 8

Tratamiento de categorías especiales de datos personales

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias, o la afiliación sindical, así como el tratamiento de datos genéticos o de datos relativos a la salud o a la vida sexual.

2. El apartado 1 no será aplicable cuando:

   a) el tratamiento esté autorizado por una ley que establezca garantías apropiadas; o

   b) el tratamiento sea necesario para proteger los intereses vitales del interesado o de otra persona; o

   c) el tratamiento ataña a datos que el interesado ha hecho manifiestamente públicos.

Artículo 9

Medidas basadas en la elaboración de perfiles y el tratamiento automatizado

1. Los Estados miembros dispondrán que las medidas que produzcan efectos jurídicos negativos para el interesado o le afecten sustancialmente y que se basen únicamente en un tratamiento automatizado de datos personales destinado a evaluar determinados aspectos personales del interesado estarán prohibidas, salvo que estén autorizadas por una ley que también establezca medidas para salvaguardar los intereses legítimos del interesado.

2. El tratamiento automatizado de datos personales destinado a evaluar determinados aspectos personales del interesado no se basará únicamente en las categorías especiales de datos personales contempladas en el artículo 8.

CAPÍTULO III

DERECHOS DEL INTERESADO

Artículo 10

Modalidades de ejercicio de los derechos del interesado

1. Los Estados miembros dispondrán que el responsable del tratamiento adoptará todas las medidas razonables para dotarse de políticas transparentes y fácilmente accesibles por lo que respecta al tratamiento de datos personales y al ejercicio de los derechos de los interesados.

2. Los Estados miembros dispondrán que el responsable del tratamiento facilitará al interesado cualquier información y comunicación relativa al tratamiento de datos personales, en forma inteligible, utilizando un lenguaje claro y sencillo.

3. Los Estados miembros dispondrán que el responsable del tratamiento adoptará todas las medidas razonables con miras a establecer procedimientos para facilitar la información contemplada en el artículo 11, y para el ejercicio de los derechos de los interesados contemplados en los artículos 12 a 17.

4. Los Estados miembros dispondrán que el responsable del tratamiento informará al interesado, sin demora injustificada, sobre el curso dado a su solicitud.

5. Los Estados miembros dispondrán que la información y cualquier medida adoptada por el responsable del tratamiento a raíz de una solicitud contemplada en los apartados 3 y 4 serán gratuitas. Cuando las solicitudes sean abusivas, en particular a causa de su carácter repetitivo, su tamaño o su volumen, el responsable del tratamiento podrá cobrar una tasa para facilitar la información o adoptar la medida solicitada, o podrá decidir no adoptar la medida solicitada. En tal caso, la carga de demostrar el carácter abusivo de la solicitud recaerá en el responsable del tratamiento.

Artículo 11
Información al interesado

1. Cuando se recojan datos personales relativos a un interesado, los Estados miembros velarán por que el responsable del tratamiento tome todas las medidas oportunas para facilitar al interesado, al menos, la siguiente información:

   a) la identidad y los datos de contacto del responsable del tratamiento y del delegado de protección de datos;

   b) los fines del tratamiento a que se destinan los datos personales;

   c) el plazo durante el cual se conservarán los datos personales;

   d) la existencia del derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, su supresión o la limitación de su tratamiento;

   e) el derecho a presentar una reclamación ante la autoridad de control contemplada en el artículo 39 y los datos de contacto de la misma;

   f) los destinatarios o las categorías de destinatarios de los datos personales, en particular en terceros países u organizaciones internacionales;

   g) cualquier otra información en la medida en que resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado, habida cuenta de las circunstancias específicas en las que se traten los datos personales.

2. Cuando los datos personales se recojan del interesado, el responsable del tratamiento le comunicará, además de la información contemplada en el apartado 1, si el suministro de datos personales es obligatorio o voluntario, así como las posibles consecuencias de que no se faciliten tales datos.

3. El responsable del tratamiento facilitará la información contemplada en el apartado 1:

   a) en el momento en que los datos personales se obtengan del interesado, o

   b) cuando los datos personales no se recojan del interesado, en el momento del registro o en un plazo razonable después de la recogida, habida cuenta de las circunstancias específicas en que se traten los datos.

4. Los Estados miembros podrán adoptar medidas legislativas por las que se retrase, limite o exima la puesta a disposición del interesado de la información en la medida y siempre que dicha limitación total o parcial constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los intereses legítimos de la persona en cuestión:

   a) para evitar que se obstaculicen pesquisas, investigaciones o procedimientos jurídicos o de carácter oficial;

b) para evitar que se prejuzgue la prevención, detección, investigación y enjuiciamiento de infracciones penales o para la ejecución de sanciones penales;

c) para proteger la seguridad pública;

d) para proteger la seguridad nacional;

e) para proteger los derechos y libertades de otras personas.

5. Los Estados miembros podrán determinar las categorías de tratamiento de datos que pueden acogerse, en su totalidad o en parte, a las exenciones del apartado 4.

Artículo 12
Derecho de acceso del interesado

1. Los Estados miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen. En caso de que se confirme el tratamiento, el responsable facilitará la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a quienes se han comunicado los datos personales, en particular los destinatarios establecidos en terceros países;

d) el plazo durante el cual se conservarán los datos personales;

e) la existencia del derecho a solicitar del responsable del tratamiento la rectificación, supresión o limitación del tratamiento de datos personales relativos al interesado;

f) el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma;

g) la comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen;

2. Los Estados miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento.

Artículo 13
Limitaciones al derecho de acceso

1. Los Estados miembros podrán adoptar medidas legislativas por las que se limite, en su totalidad o en parte, el derechos de acceso del interesado en la medida en que dicha limitación parcial o completa constituya una medida necesaria y proporcional

en una sociedad democrática, teniendo debidamente en cuenta los intereses legítimos de la persona de que se trate:

a) para evitar que se obstaculicen pesquisas, investigaciones o procedimientos jurídicos u oficiales;

b) para evitar que se prejuzgue la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales;

c) para proteger la seguridad pública;

d) para proteger la seguridad nacional;

e) para proteger los derechos y libertades de otras personas.

2. Los Estados miembros podrán determinar por ley las categorías de tratamiento de datos que pueden acogerse en todo o en parte a las exenciones del apartado 1.

3. En los casos contemplados en los apartados 1 y 2, los Estados miembros dispondrán que el responsable del tratamiento informará por escrito al interesado sobre cualquier denegación o limitación de acceso, sobre las razones de la denegación y sobre las posibilidades de presentar a la autoridad de control una reclamación e interponer un recurso judicial. La información sobre los fundamentos de hecho o de Derecho en los que se sustenta la decisión podrá omitirse cuando el suministro de dicha información pueda comprometer uno de los fines contemplados en el apartado 1.

4. Los Estados miembros velarán por que el responsable del tratamiento documente los motivos por los que no comunicó los fundamentos de hecho o de Derecho en los que se sustenta la decisión.

Artículo 14
Modalidades de ejercicio del derecho de acceso

1. Los Estados miembros reconocerán el derecho del interesado a solicitar, en particular en los casos contemplados en el artículo 13, que la autoridad de control compruebe la licitud del tratamiento.

2. Los Estados miembros dispondrán que el responsable del tratamiento informará al interesado del derecho a solicitar la intervención de las autoridades de control con arreglo a lo dispuesto en el apartado 1.

3. Cuando se ejerza el derecho contemplado en el apartado 1, la autoridad de control informará al interesado, al menos, de que se han llevado a cabo todas las verificaciones necesarias, así como del resultado en lo tocante a la licitud del tratamiento en cuestión.

Artículo 15

Derecho de rectificación

1. Los Estados miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento la rectificación de los datos personales que le conciernen cuando tales datos resulten inexactos. El interesado tendrá derecho a que se completen los datos personales cuando estos resulten incompletos, en particular mediante una declaración rectificativa.

2. Los Estados miembros dispondrán que el responsable del tratamiento informará por escrito al interesado sobre cualquier denegación de rectificación, sobre las razones de la denegación y sobre las posibilidades de presentar una reclamación ante la autoridad de control y de interponer un recurso judicial.

Artículo 16

Derecho de supresión

1. Los Estados miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento la supresión de los datos personales que le conciernen cuando el tratamiento no cumpla las disposiciones adoptadas con arreglo al artículo 4, letras a) a e), y a los artículos 7 y 8 de la presente Directiva.

2. El responsable del tratamiento procederá a la supresión sin demora.

3. En lugar de proceder a la supresión, el responsable del tratamiento marcará los datos personales cuando:

   a) el interesado impugne su exactitud, durante un plazo que permita al responsable del tratamiento verificar la exactitud de dichos datos;

   b) los datos personales hayan de conservarse a efectos probatorios;

   c) el interesado se oponga a su supresión y solicite la limitación de su uso.

4. Los Estados miembros dispondrán que el responsable del tratamiento informará por escrito al interesado de cualquier denegación de la supresión o marcado del tratamiento, las razones de la denegación y las posibilidades de presentar una reclamación ante la autoridad de control y de interponer un recurso judicial.

Artículo 17

Derechos del interesado en las investigaciones y los procedimientos penales

Los Estados miembros dispondrán que los derechos de información, acceso, rectificación, supresión y limitación del tratamiento contemplados en los artículos 11 a 16 se ejercerán de conformidad con las normas nacionales de enjuiciamiento cuando los datos personales figuren en una resolución judicial o en un registro tratado en el curso de investigaciones y procedimientos penales.

CAPÍTULO IV
RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

SECCIÓN 1
OBLIGACIONES GENERALES

Artículo 18

Obligaciones del responsable del tratamiento

1. Los Estados miembros dispondrán que el responsable del tratamiento adoptará políticas e implementará medidas apropiadas para asegurar que el tratamiento de datos personales se lleva a cabo de conformidad con las disposiciones adoptadas con arreglo a la presente Directiva.

2. Las medidas previstas en el apartado 1 incluirán, en particular:

   a) la conservación de la documentación con arreglo a lo dispuesto en el artículo 23;

   b) el cumplimiento de los requisitos en materia de consulta previa de conformidad con lo dispuesto en el artículo 26;

   c) la implementación de los requisitos en materia de seguridad de los datos establecidos en el artículo 27;

   d) la designación de un delegado de protección de datos con arreglo a lo dispuesto en el artículo 30.

3. El responsable del tratamiento implementará mecanismos para verificar la eficacia de las medidas contempladas en el apartado 1. Siempre que no sea desproporcionado, estas verificaciones serán llevadas a cabo por auditores independientes internos o externos.

Artículo 19

Protección de datos desde el diseño y protección de datos por defecto

1. Los Estados miembros dispondrán que, habida cuenta de las técnicas existentes y de los costes asociados a su implementación, el responsable del tratamiento implementará medidas y procedimientos técnicos y organizativos apropiados, de manera que el tratamiento sea conforme con las disposiciones adoptadas con arreglo a la presente Directiva y garantice la protección de los derechos del interesado.

2. El responsable del tratamiento implementará mecanismos con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para los fines del tratamiento.

Artículo 20
Corresponsables del tratamiento

Los Estados miembros dispondrán que cuando un responsable del tratamiento determine, conjuntamente con otros, los fines, las condiciones y los medios del tratamiento de datos personales, los corresponsables deben determinar, de mutuo acuerdo, cuáles son sus responsabilidades respectivas en el cumplimiento de las disposiciones adoptadas con arreglo a la presente Directiva, en particular por lo que hace a los procedimientos y mecanismos para el ejercicio de los derechos del interesado.

Artículo 21
Encargado del tratamiento

1. Los Estados miembros dispondrán que cuando una operación de tratamiento sea llevada a cabo por cuenta de un responsable del tratamiento, este debe elegir un encargado del tratamiento que ofrezca garantías suficientes para implementar medidas y procedimientos técnicos y organizativos apropiados, de manera que el tratamiento sea conforme con los requisitos de las disposiciones adoptadas con arreglo a la presente Directiva y asegure la protección de los derechos del interesado.

2. Los Estados miembros dispondrán que la realización del tratamiento por un encargado debe regirse por un acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento y que disponga, en particular, que el encargado del tratamiento actuará únicamente siguiendo las instrucciones del responsable del tratamiento, en particular cuando la transferencia de los datos personales utilizados esté prohibida.

3. Si un encargado del tratamiento trata datos personales sin seguir las instrucciones del responsable del tratamiento, el encargado será considerado responsable del tratamiento con respecto a ese tratamiento y estará sujeto a las normas aplicables a los corresponsables del tratamiento establecidas en el artículo 20.

Artículo 22
Tratamiento bajo la autoridad del responsable y del encargado del tratamiento

Los Estados miembros dispondrán que el encargado del tratamiento, así como cualquier persona que actúe bajo la autoridad del responsable o del encargado del tratamiento, que tenga acceso a datos personales solo podrá someterlos a tratamiento siguiendo instrucciones del responsable del tratamiento o cuando así lo requiera el Derecho de la Unión o de un Estado miembro.

Artículo 23
Documentación

1. Los Estados miembros dispondrán que cada responsable y cada encargado del tratamiento conservarán la documentación de todas los procedimientos y sistemas de tratamiento bajo su responsabilidad.

2. La documentación deberá contener, como mínimo, la información siguiente:

a) el nombre y los datos de contacto del responsable del tratamiento o de cualquier corresponsable o coencargado del tratamiento;

b) los fines del tratamiento;

c) los destinatarios o las categorías de destinatarios de los datos personales;

d) las transferencias de datos a un tercer país o a una organización internacional, incluido el nombre de dicho tercer país o de dicha organización internacional.

3. El responsable y el encargado del tratamiento pondrán la documentación a disposición de la autoridad de control, a solicitud de esta.

Artículo 24
Llevanza de registros

1. Los Estados miembros velarán por que se lleven registros de, al menos, las operaciones de tratamiento siguientes: recogida, alteración, consulta, comunicación, combinación o supresión. Los registros de consulta y comunicación mostrarán, en particular, el fin, la fecha y la hora de tales operaciones y, en la medida de lo posible, el nombre de la persona que consultó o comunicó datos personales.

2. Los registros se utilizarán únicamente a efectos de comprobación de la licitud del tratamiento y de autocontrol, así como para asegurar la integridad y la seguridad de los datos.

Artículo 25
Cooperación con la autoridad de control

1. Los Estados miembros dispondrán que el responsable y el encargado del tratamiento cooperarán con la autoridad de control en el desempeño de las funciones de esta, en particular facilitando toda la información necesaria al efecto.

2. Cuando la autoridad de control ejerza los poderes que le son conferidos en virtud de las letras a) y b) del artículo 46, el responsable y el encargado del tratamiento responderán a la autoridad de control dentro de un plazo razonable. La respuesta deberá incluir una descripción de las medidas adoptadas y los resultados obtenidos, en respuesta a las observaciones formuladas por la autoridad de control.

Artículo 26
Consulta previa de la autoridad de control

1. Los Estados miembros velarán por que el responsable o el encargado del tratamiento consulten a la autoridad de control antes de proceder al tratamiento de datos personales que vayan a formar parte de un nuevo sistema de archivo que haya de crearse, cuando:

a) vayan a tratarse categorías especiales de datos contempladas en el artículo 8;

b) el tipo de tratamiento, en particular cuando se usen tecnologías, mecanismos o procedimientos nuevos, entrañe riesgos específicos para los derechos y libertades fundamentales y, en particular, para la protección de datos personales de los interesados.

2. Los Estados miembros podrán disponer que la autoridad de control establecerá una lista de las operaciones de tratamiento que están sujetas a consulta previa con arreglo a lo dispuesto en el apartado 1.

SECCIÓN 2
SEGURIDAD DE LOS DATOS

Artículo 27
Seguridad del tratamiento

1. Los Estados miembros dispondrán que el responsable y el encargado del tratamiento implementarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en relación con los riesgos que entrañe el tratamiento y la naturaleza de los datos que deban protegerse, habida cuenta de las técnicas existentes y de los costes asociados a su implementación.

2. Por lo que hace al tratamiento automatizado de datos, cada Estado miembro dispondrá que el responsable o el encargado del tratamiento, a raíz de una evaluación de los riesgos, implementará medidas destinadas a:

a) denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento de datos personales (control de acceso a los equipamientos);

b) impedir que los soportes de datos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas (control de los soportes de datos);

c) impedir que se introduzcan sin autorización datos personales conservados, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización (control de la conservación);

d) impedir que los sistemas de tratamiento automatizado de datos puedan ser utilizados por personas no autorizadas por medio de equipamientos de comunicación de datos (control de los usuarios);

e) garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado de datos solo puedan tener acceso a los datos para los que han sido autorizados (control del acceso a los datos);

f) garantizar que sea posible verificar y constatar a qué organismos se han transmitido o pueden transmitirse o a cuya disposición pueden ponerse datos personales mediante equipamientos de comunicación de datos (control de las comunicaciones);

g) garantizar que pueda verificarse y constatarse *a posteriori* qué datos personales se han introducido en los sistemas de tratamiento automatizado de datos y en

qué momento y por qué persona han sido introducidos (control de la introducción);

h) impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);

i) garantizar que los sistemas instalados puedan restablecerse en caso de interrupción (recuperación);

j) garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados (fiabilidad) y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema (integridad).

3. La Comisión podrá adoptar, en caso necesario, actos de ejecución para especificar los requisitos establecidos en los apartados 1 y 2 a distintas situaciones, en particular normas de cifrado. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 57, apartado 2.

Artículo 28

Notificación de una violación de datos personales a la autoridad de control

1. Los Estados miembros dispondrán que, en caso de violación de datos personales, el responsable del tratamiento la notificará a la autoridad de control sin demora injustificada, y, de ser posible, a más tardar veinticuatro horas después de que haya tenido constancia de ella. Si la notificación no se hace en el plazo de veinticuatro horas, el responsable facilitará a la autoridad de control, previa solicitud, una justificación motivada.

2. El encargado del tratamiento alertará e informará al responsable del tratamiento inmediatamente después de que haya constatado una violación de datos personales.

3. La notificación contemplada en el apartado 1 deberá, al menos:

a) describir la naturaleza de la violación de datos personales, en particular las categorías y el número de interesados afectados, y las categorías y el número de registros de datos afectados;

b) comunicar la identidad y los datos de contacto del delegado de protección de datos contemplado en el artículo 30 o de otro punto de contacto en el que pueda obtenerse más información;

c) recomendar medidas tendentes a atenuar los posibles efectos negativos de la violación de datos personales;

d) describir las posibles consecuencias de la violación de datos personales;

e) describir las medidas propuestas o adoptadas por el responsable del tratamiento para poner remedio a la violación de datos personales.

4. Los Estados miembros dispondrán que el responsable del tratamiento documentará cualquier violación de datos personales, indicando su contexto, sus efectos y las medidas correctivas adoptadas. Esta documentación deberá permitir a la autoridad de control verificar el cumplimiento de las disposiciones del presente artículo. Solo incluirá la información necesaria a tal efecto.

5. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 56, a fin de especificar los criterios y requisitos aplicables a la constatación de la violación de datos contemplada en los apartados 1 y 2 y en relación con las circunstancias particulares en las que se exige a un responsable y un encargado del tratamiento notificar la violación de datos personales.

6. La Comisión podrá definir el formato normalizado de dicha notificación a la autoridad de control, los procedimientos aplicables al requisito de notificación y la forma y las modalidades de la documentación contemplada en el apartado 4, incluidos los plazos para la supresión de la información que figura en ella. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 57, apartado 2.

Artículo 29
Comunicación de una violación de datos personales al interesado

1. Los Estados miembros dispondrán que, cuando sea probable que la violación de datos personales afecte negativamente a la protección de los datos personales o la privacidad del interesado, el responsable del tratamiento, después de haber procedido a la notificación contemplada en el artículo 28, comunicará al interesado, sin demora injustificada, la violación de datos personales.

2. La comunicación al interesado contemplada en el apartado 1 describirá la naturaleza de la violación de datos personales y contendrá, al menos, la información y las recomendaciones previstas en el artículo 28, apartado 3, letras b) y c).

3. La comunicación de una violación de datos personales al interesado no será necesaria si el responsable del tratamiento demuestra, a satisfacción de la autoridad de control, que ha implementado medidas de protección tecnológica apropiadas y que estas medidas se han aplicado a los datos afectados por la violación. Dichas medidas de protección tecnológica deberán hacer ininteligibles los datos para cualquier persona que no esté autorizada a acceder a ellos.

4. La comunicación al interesado podrá aplazarse, limitarse u omitirse por los motivos contemplados en el artículo 11, apartado 4.

SECCIÓN 3
DELEGADO DE PROTECCIÓN DE DATOS

Artículo 30
Designación del delegado de protección de datos

1. Los Estados miembros dispondrán que el responsable o el encargado del tratamiento designarán un delegado de protección de datos.

2. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, y a su capacidad para ejecutar las tareas contempladas en el artículo 32.

3. El delegado de protección de datos podrá ser designado para varias entidades, teniendo en cuenta la estructura organizativa de la autoridad competente.

Artículo 31
Función de delegado de protección de datos

1. Los Estados miembros dispondrán que el responsable o el encargado del tratamiento velarán por que el delegado de protección de datos se implique adecuadamente y en su debido momento en todas las cuestiones relativas a la protección de datos personales.

2. El responsable o el encargado del tratamiento velarán por que se faciliten al delegado de protección de datos los medios para desempeñar las funciones y tareas contempladas en el artículo 32 con eficacia e independencia, y por que no reciba ninguna instrucción en lo que respecta al ejercicio de sus funciones.

Artículo 32
Tareas del delegado de protección de datos

Los Estados miembros dispondrán que el responsable o el encargado del tratamiento encomendarán al delegado de protección de datos, como mínimo, las siguientes tareas:

a) informar y asesorar al responsable o al encargado del tratamiento de las obligaciones que les incumben de conformidad con las disposiciones adoptadas en virtud de la presente Directiva, y documentar esta actividad y las respuestas recibidas;

b) supervisar la implementación y aplicación de las políticas relativas a la protección de datos personales, incluida la asignación de responsabilidades, la formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) supervisar la implementación y aplicación de las disposiciones adoptadas en virtud de la presente Directiva, en particular por lo que hace a los requisitos relativos a la protección de datos desde el diseño, la protección de datos por defecto y la seguridad de los datos, así como a la información de los interesados y las solicitudes presentadas en el ejercicio de sus derechos en virtud de las disposiciones adoptadas con arreglo a la presente Directiva;

d) velar por la conservación de la documentación contemplada en el artículo 23;

e) supervisar la documentación, notificación y comunicación de las violaciones de datos personales con arreglo a lo dispuesto en los artículos 28 y 29;

f) supervisar la presentación de solicitudes de consulta previa a la autoridad de control, si así se requiere de conformidad con lo dispuesto en el artículo 26;

g) supervisar la respuesta a las solicitudes de la autoridad de control y, en el marco de la competencia del delegado de protección de datos, cooperar con la autoridad de control a solicitud de esta o a iniciativa propia;

h) actuar como punto de contacto para la autoridad de control sobre las cuestiones relacionadas con el tratamiento y consultar a la autoridad de control, si procede, a iniciativa propia.

CAPÍTULO V
TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

Artículo 33
Principios generales de las transferencias de datos personales

Los Estados miembros dispondrán que cualquier transferencia de datos personales por las autoridades competentes que sean o vayan a ser objeto de tratamiento tras su transferencia a un tercer país o a una organización internacional, incluidas las transferencias ulteriores a otro tercer país u otra organización internacional, solo podrá realizarse si:

a) la transferencia es necesaria para la prevención, investigación, detección o enjuiciamiento de infracciones penales o para la ejecución de sanciones penales; y

b) el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo.

Artículo 34
Transferencias con una decisión de adecuación

1. Los Estados miembros dispondrán que una transferencia de datos personales a un tercer país o una organización internacional podrá realizarse cuando la Comisión haya decidido, de conformidad con lo dispuesto en el artículo 41 del Reglamento (UE) nº …./2012 o de conformidad con el apartado 3 del presente artículo, que el tercer país, o un territorio o un sector de tratamiento en ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dichas transferencias no requerirán nuevas autorizaciones.

2. Cuando no exista una decisión adoptada de conformidad con lo dispuesto en el artículo 41 del Reglamento (UE) nº …./2012, la Comisión evaluará la adecuación del nivel de protección, tomando en consideración los elementos siguientes:

a) el Estado de Derecho, la legislación pertinente en vigor, tanto general como sectorial, en particular en lo que respecta a la seguridad pública, la defensa, la seguridad nacional, el Derecho penal, las medidas de seguridad en vigor en el país de que se trate o aplicables a la organización internacional en cuestión, así como los derechos efectivos y exigibles, incluido el derecho de recurso administrativo y judicial efectivo de los interesados, en particular los residentes en la Unión cuyos datos personales estén siendo transferidos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país u organización internacional de que se trate, encargadas de garantizar el cumplimiento de las normas en materia de protección de datos, de asistir y asesorar a los interesados en el ejercicio de sus derechos y de cooperar con las autoridades de control de la Unión y de los Estados miembros; y

c) los compromisos internacionales asumidos por el tercer país o la organización internacional de que se trate.

3. La Comisión podrá decidir, dentro del ámbito de aplicación de la presente Directiva, que un tercer país, o un territorio o un sector de tratamiento de datos en ese tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 57, apartado 2.

4. El acto de ejecución especificará su ámbito de aplicación geográfica y sectorial, y, cuando proceda, determinará cuál es la autoridad de control mencionada en el apartado 2, letra b).

5. La Comisión podrá decidir, dentro del ámbito de aplicación de la presente Directiva, que un tercer país, o un territorio o un sector de tratamiento de datos en ese tercer país, o una organización internacional no garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2, en particular en los casos en que la legislación pertinente, tanto general como sectorial, en vigor en el tercer país o aplicable a la organización internacional en cuestión, no garantice derechos efectivos y exigibles, incluido el derecho de recurso administrativo y judicial efectivo de los interesados, en particular aquellos cuyos datos personales estén siendo transferidos. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen contemplado en el artículo 57, apartado 2, o, en casos de extrema urgencia para personas en lo que respecta a su derecho a la protección de datos personales, de conformidad con el procedimiento contemplado en el artículo 57, apartado 3.

6. Los Estados miembros velarán por que cuando la Comisión adopte una decisión de conformidad con lo dispuesto en el apartado 5, esté prohibida toda transferencia de datos personales al tercer país, o a un territorio o un sector de tratamiento de datos en ese tercer país, o a la organización internacional de que se trate; dicha decisión se entenderá sin perjuicio de las transferencias en virtud del artículo 35, apartado 1, o de conformidad con lo dispuesto en el artículo 36. La Comisión entablará consultas, en su debido momento, con el tercer país o la organización internacional con vistas a poner remedio a la situación resultante de la decisión adoptada de conformidad con lo dispuesto en el apartado 5 del presente artículo.

7. La Comisión publicará en el *Diario Oficial de la Unión Europea* una lista de los terceros países, territorios y sectores de tratamiento de datos en un tercer país o una organización internacional para los que haya decidido que está o no está garantizado un nivel protección adecuado.

8. La Comisión supervisará la aplicación de los actos de ejecución contemplados en los apartados 3 y 5.

Artículo 35
Transferencias mediante garantías apropiadas

1. Cuando la Comisión no haya adoptado una decisión con arreglo a lo dispuesto en el artículo 34, los Estados miembros dispondrán que podrá tener lugar una transferencia de datos personales a un destinatario en un tercer país o una organización internacional cuando:

   a) se hayan aportado garantías apropiadas con respecto a la protección de datos personales en un instrumento jurídicamente vinculante; o

   b) el responsable o el encargado del tratamiento hayan evaluado todas las circunstancias que concurren en la transferencia de datos personales y hayan llegado a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales.

2. La decisión relativa a una transferencia en virtud del apartado 1, letra b), deberá ser adoptada por personal debidamente autorizado. Estas transferencias deberán documentarse y la documentación se pondrá a disposición, previa solicitud, de la autoridad de control.

Artículo 36
Excepciones

No obstante lo dispuesto en los artículos 34 y 35, los Estados miembros dispondrán que solo podrá procederse a la transferencia de datos personales a un tercer país o una organización internacional en caso de que:

a) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otra persona; o

b) la transferencia sea necesaria para salvaguardar intereses legítimos del interesado cuando así lo disponga el Derecho del Estado miembro que transfiere los datos personales; o

c) la transferencia de los datos sea esencial para prevenir una amenaza inminente y grave para la seguridad pública de un Estado miembro o de un tercer país; o

d) la transferencia sea necesaria en casos concretos a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales; o

e) la transferencia sea necesaria en casos concretos para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial relativo a la prevención, investigación, detección o enjuiciamiento de una infracción penal o la ejecución de una sanción penal específica.

Artículo 37

Condiciones específicas para la transferencia de datos personales

Los Estados miembros dispondrán que el responsable del tratamiento informará al destinatario de los datos personales de cualquier limitación al tratamiento y tomará todas las medidas razonables para garantizar que se cumplan dichas limitaciones.

Artículo 38

Cooperación internacional en el ámbito de la protección de datos personales

1. En relación con los terceros países y las organizaciones internacionales, la Comisión y los Estados miembros tomarán medidas apropiadas para:

   a) crear mecanismos de cooperación internacional eficaces que faciliten la aplicación de la legislación relativa a la protección de datos personales;

   b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías apropiadas para la protección de los datos personales y otros derechos y libertades fundamentales;

   c) procurar la participación de las partes interesadas pertinentes en los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

   d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales.

2. A efectos de la aplicación del apartado 1, la Comisión tomará medidas apropiadas para impulsar las relaciones con terceros países u organizaciones internacionales y, en particular, sus autoridades de control, cuando haya decidido que garantizan un nivel de protección adecuado a tenor de lo dispuesto en el artículo 34, apartado 3.

CAPÍTULO VI
AUTORIDADES DE CONTROL INDEPENDIENTES

SECCIÓN 1
INDEPENDENCIA

Artículo 39

Autoridad de control

1. Cada Estado miembro dispondrá que una o varias autoridades públicas se encargarán de supervisar la aplicación de las disposiciones adoptadas con arreglo a la presente Directiva y de contribuir a su aplicación coherente en toda la Unión, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento de sus datos personales y de facilitar la libre circulación de

datos personales en la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión.

2. Los Estados miembros podrán disponer que las autoridades de control creadas en los Estados miembros de conformidad con lo dispuesto en el Reglamento (UE) nº …./2012 asumirán las tareas de la autoridad de control que vaya a crearse de conformidad con el apartado 1.

3. Cuando en un Estado miembro estén establecidas varias autoridades de control, dicho Estado miembro designará la autoridad de control que actuará como punto de contacto único, a fin de favorecer la participación efectiva de dichas autoridades en el Consejo Europeo de Protección de Datos.

Artículo 40
Independencia

1. Los Estados miembros velarán por que la autoridad de control actúe con total independencia en el ejercicio de las funciones que le hayan sido encomendadas y de los poderes que le hayan sido conferidos.

2. Cada Estado miembro dispondrá que, en el ejercicio de sus funciones, los miembros de la autoridad de control no solicitarán ni aceptarán instrucciones de nadie.

3. Los miembros de la autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada.

4. Tras la finalización de su mandato, los miembros de la autoridad de control actuarán con integridad y discreción en lo que respecta a la aceptación de cargos y beneficios.

5. Cada Estado miembro velará por que la autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros adecuados, así como de las instalaciones e infraestructuras necesarias para el ejercicio efectivo de sus funciones y poderes, en particular aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación activa en el Consejo Europeo de Protección de Datos.

6 Cada Estado miembro velará por que la autoridad de control disponga de su propio personal, que será nombrado por el director de la autoridad de control y estará sujeto a su autoridad.

7. Los Estados miembros velarán por que la autoridad de control esté sujeta a control financiero, sin que ello afecte a su independencia. Los Estados miembros velarán por que la autoridad de control disponga de presupuestos anuales propios. Los presupuestos se harán públicos.

Artículo 41

Condiciones generales aplicables a los miembros de la autoridad de control

1. Los Estados miembros dispondrán que los miembros de la autoridad de control deben ser nombrados bien por su parlamento bien por su gobierno.

2. Los miembros serán elegidos entre personas que ofrezcan absolutas garantías de independencia y que posean experiencia y aptitudes acreditadas para el ejercicio de sus funciones.

3. Las funciones de los miembros terminarán a la expiración de su mandato o, en caso de dimisión o jubilación obligatoria, de conformidad con lo dispuesto en el apartado 5.

4. Un miembro podrá ser destituido o desposeído de su derecho a pensión u otros beneficios sustitutivos por el órgano jurisdiccional nacional competente si dejara de reunir las condiciones necesarias para el ejercicio de sus funciones o hubiera incurrido en falta grave.

5. Un miembro cuyo mandato expire o que presente su dimisión seguirá ejerciendo sus funciones hasta que se nombre un nuevo miembro.

Artículo 42

Normas relativas al establecimiento de la autoridad de control

Cada Estado miembro dispondrá por ley:

a) el establecimiento y el estatuto de la autoridad de control con arreglo a lo dispuesto en los artículos 39 y 40;

b) las cualificaciones, la experiencia y las aptitudes requeridas para ejercer las funciones de miembro de la autoridad de control;

c) las normas y los procedimientos para el nombramiento de los miembros de la autoridad de control, así como las normas relativas a las actividades u ocupaciones incompatibles con sus funciones;

d) la duración del mandato de los miembros de la autoridad de control, que no será inferior a cuatro años, salvo los primeros nombramientos tras la entrada en vigor de la presente Directiva, algunos de los cuales podrán ser más breves;

e) el carácter renovable o no renovable del mandato de los miembros de la autoridad de control;

f) las reglas y condiciones comunes que rigen las funciones de los miembros y del personal de la autoridad de control;

g) las normas y los procedimientos relativos al cese de las funciones de los miembros de la autoridad de control, en particular cuando hayan dejado de cumplir las condiciones requeridas para el ejercicio de sus funciones o incurrieran en falta grave.

Artículo 43
Secreto profesional

Los Estados miembros dispondrán que los miembros y el personal de la autoridad de control estarán sujetos, tanto durante su mandato como después del mismo, al deber de secreto profesional con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el ejercicio de sus funciones oficiales.

SECCIÓN 2
FUNCIONES Y PODERES

Artículo 44
Competencia

1. Los Estados miembros dispondrán que cada autoridad de control ejercerá, en el territorio de su propio Estado miembro, los poderes que se le confieran de conformidad con la presente Directiva.

2. Los Estados miembros dispondrán que la autoridad de control no será competente para controlar las operaciones de tratamiento efectuadas por los órganos jurisdiccionales en el ejercicio de su función jurisdiccional.

Artículo 45
Funciones

1. Los Estados miembros dispondrán que la autoridad de control:

   a) supervisará y asegurará la aplicación de las disposiciones adoptadas con arreglo a la presente Directiva y sus medidas de ejecución;

   b) conocerá las reclamaciones presentadas por cualquier interesado o por una asociación que le represente y que esté debidamente autorizada por él de conformidad con lo dispuesto en el artículo 50, investigará, en la medida en que proceda, el asunto e informará al interesado o la asociación sobre el curso y el resultado de la reclamación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

   c) controlará la licitud del tratamiento de datos con arreglo a lo dispuesto en el artículo 14, e informará al interesado, en un plazo razonable, sobre el resultado del control o sobre los motivos por los que no se ha llevado a cabo;

   d) prestará asistencia mutua a otras autoridades de control y garantizará la coherencia de la aplicación y el cumplimiento de las disposiciones adoptadas con arreglo a la presente Directiva;

   e) llevará a cabo investigaciones, ya sea a iniciativa propia, ya sea a raíz de una reclamación o a solicitud de otra autoridad de control, e informará al interesado

en cuestión, si este hubiera presentado una reclamación, del resultado de las investigaciones en un plazo razonable;

f) hará un seguimiento de las novedades de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación;

g) será consultado por las instituciones y los organismos de los Estados miembros sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales;

h) será consultado sobre las operaciones de tratamiento de datos con arreglo al artículo 26;

i) participará en las actividades del Consejo Europeo de Protección de Datos.

2. Cada autoridad de control promoverá la sensibilización del público sobre los riesgos, normas, garantías y derechos relativos al tratamiento de datos personales. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención.

3. La autoridad de control, previa solicitud, asesorará a cualquier interesado en el ejercicio de los derechos que confieren disposiciones adoptadas con arreglo a la presente Directiva y, en su caso, cooperará a tal fin con las autoridades de control de otros Estados miembros.

4. Para las reclamaciones contempladas en el apartado 1, letra b), la autoridad de control facilitará un formulario de reclamaciones que podrá cumplimentarse por vía electrónica, sin excluir otros medios de comunicación.

5. Los Estados miembros dispondrán que el desempeño de las funciones de la autoridad de control será gratuito para el interesado.

6. Cuando las solicitudes sean abusivas, en particular por su carácter repetitivo, la autoridad de control podrá exigir el pago de una tasa o decidir no adoptar las medidas solicitadas por el interesado. La carga de la prueba del carácter abusivo de la solicitud recaerá en la autoridad de control.

Artículo 46
Poderes

Los Estados miembros dispondrán que cada autoridad de control deberá estar investida, en particular, de:

a) poderes de investigación, como el poder de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;

b) poderes efectivos de intervención, por ejemplo para emitir dictámenes antes de que se lleve a cabo el tratamiento, y garantizar una publicación adecuada de

dichos dictámenes, ordenar la limitación, supresión o destrucción de datos, imponer una prohibición temporal o definitiva del tratamiento, formular una advertencia o una amonestación al responsable de la misma, o remitir el asunto a los parlamentos nacionales u otras instituciones políticas;

c) el poder de emprender acciones legales cuando se hayan infringido las disposiciones adoptadas con arreglo a la presente Directiva o de denunciar dichas infracciones a las autoridades judiciales.

Artículo 47
Informe de actividad

Los Estados miembros dispondrán que cada autoridad de control elaborará un informe anual sobre sus actividades. El informe se pondrá a disposición de la Comisión y el Consejo Europeo de Protección de Datos.

CAPÍTULO VII
COOPERACIÓN

Artículo 48
Asistencia mutua

1. Los Estados miembros dispondrán que las autoridades de control se prestarán asistencia mutua a fin de implementar y aplicar las disposiciones adoptada con arreglo a la presente Directiva de forma coherente, y tomarán medidas para asegurar una efectiva cooperación entre sí. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como, por ejemplo, las solicitudes para llevar a cabo consultas previas, inspecciones e investigaciones.

2. Los Estados miembros dispondrán que una autoridad de control adoptará todas las medidas apropiadas requeridas para responder a la solicitud de otra autoridad de control.

3. La autoridad de control a la que se haya dirigido una solicitud de asistencia informará a la autoridad de control solicitante de los resultados obtenidos o, en su caso, de los progresos registrados o de las medidas adoptadas para dar curso a su solicitud.

Artículo 49
Tareas del Consejo Europeo de Protección de Datos

1. El Consejo Europeo de Protección de datos creado por el Reglamento (UE) nº …./2012 ejercerá, dentro del ámbito de aplicación de la presente Directiva, las siguientes tareas en relación con el tratamiento de datos:

a) asesorará a la Comisión sobre cualquier cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación de la presente Directiva;

b) examinará, a solicitud de la Comisión o a iniciativa propia o de uno de sus miembros, cualquier cuestión relativa a la aplicación de las disposiciones adoptadas con arreglo a la presente Directiva y emitirá directrices, recomendaciones y mejores prácticas dirigidas a las autoridades de control, a fin de promover la aplicación coherente de esas disposiciones;

c) examinará la aplicación práctica de las directrices, recomendaciones y mejores prácticas contempladas en la letra b) e informará de ellas periódicamente a la Comisión;

d) emitirá un dictamen destinado a la Comisión sobre el nivel de protección en terceros países u organizaciones internacionales;

e) promoverá la cooperación y los intercambios bilaterales y multilaterales efectivos de información y de prácticas entre las autoridades de control;

f) promoverá programas de formación comunes y facilitará los intercambios de personal entre las autoridades de control, así como, cuando proceda, con las autoridades de control de terceros países o de organizaciones internacionales;

g) promoverá el intercambio de conocimientos y documentación con las autoridades de control de la protección de datos a escala mundial, en particular sobre la legislación y las prácticas en materia de protección de datos.

2. Cuando la Comisión solicite asesoramiento del Consejo Europeo de Protección de Datos podrá fijar un plazo para la prestación de dicho asesoramiento, teniendo en cuenta la urgencia del asunto.

3. El Consejo Europeo de Protección de Datos transmitirá sus dictámenes, directrices, recomendaciones y mejores prácticas a la Comisión y al Comité contemplado en el artículo 57, apartado 1, y los hará públicos.

4. La Comisión informará al Consejo Europeo de Protección de Datos de las medidas que haya adoptado siguiendo los dictámenes, directrices, recomendaciones y mejores prácticas emitidos por dicho Consejo.

CAPÍTULO VIII
RECURSOS, RESPONSABILIDAD Y SANCIONES

Artículo 50
Derecho a presentar una reclamación ante una autoridad de control

1. Sin perjuicio de los recursos administrativos o judiciales, los Estados miembros reconocerán el derecho que asiste a todo interesado a presentar una reclamación ante la autoridad de control de cualquier Estado miembro si considera que el tratamiento de sus datos personales no se ajusta a las disposiciones adoptadas con arreglo a la presente Directiva.

2. Los Estados miembros reconocerán el derecho que asiste a todo organismo, organización o asociación que tenga por objeto proteger los derechos e intereses de los interesados por lo que se refiere a la protección de sus datos personales, y que

haya sido correctamente constituido con arreglo a la legislación de un Estado miembro, a presentar una reclamación ante una autoridad de control en cualquier Estado miembro por cuenta de uno o más interesados si considera que los derechos que le asisten en virtud de la presente Directiva han sido vulnerados como consecuencia del tratamiento de datos personales. La organización o asociación deberá estar debidamente autorizada por el interesado o interesados.

3. Los Estados miembros reconocerán el derecho que asiste a todo organismo, organización o asociación contemplado en el apartado 2, independientemente de la reclamación de un interesado, a presentar una reclamación ante una autoridad de control en cualquier Estado miembro si considera que se ha producido una violación de los datos personales.

Artículo 51
Derecho a un recurso judicial contra una autoridad de control

1. Los Estados miembros reconocerán el derecho a un recurso judicial contra las decisiones de una autoridad de control.

2. Cada interesado tendrá derecho a un recurso judicial que obligue a la autoridad de control a dar curso a una reclamación en ausencia de una decisión necesaria para proteger sus derechos, o en caso de que la autoridad de control no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación con arreglo a lo dispuesto en el artículo 45, apartado 1, letra b).

3. Los Estados miembros dispondrán que las acciones legales contra una autoridad de control deberán ejercitarse antes los órganos jurisdiccionales del Estado miembro en que esté establecida la autoridad de control.

Artículo 52
Derecho a un recurso judicial contra un responsable o encargado

Sin perjuicio de los recursos administrativos disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control, los Estados miembros reconocerán el derecho que asiste a toda persona física a interponer un recurso judicial si considera que sus derechos establecidos en disposiciones adoptadas con arreglo a la presente Directiva han sido vulnerados como consecuencia de un tratamiento de sus datos personales no conforme con esas disposiciones.

Artículo 53
Normas comunes para los procedimientos judiciales

1. Los Estados miembros reconocerán el derecho que asiste a todo organismo, organización o asociación a que se refiere el artículo 50, apartado 2, a ejercer los derechos contemplados en los artículos 51 y 52 en nombre de uno o más interesados.

2. Las autoridades de control tendrán derecho a litigar y ejercitar acciones ante un órgano jurisdiccional con el fin de garantizar el cumplimiento de las disposiciones

adoptadas con arreglo a la presente Directiva o de garantizar la coherencia de la protección de los datos personales en el territorio de la Unión.

3. Los Estados miembros velarán por que las acciones jurisdiccionales existentes en virtud de la legislación nacional permitan la rápida adopción de medidas, incluso medidas provisionales, destinadas a poner término a cualquier presunta infracción y a evitar que se produzcan nuevos perjuicios contra los intereses afectados.

Artículo 54
Responsabilidad y derecho a indemnización

1. Los Estados miembros dispondrán que toda persona que haya sufrido un perjuicio como consecuencia de una operación de tratamiento ilícito o de un acto incompatible con las disposiciones adoptadas con arreglo a la presente Directiva tendrá derecho a recibir del responsable o encargado del tratamiento una indemnización por el perjuicio sufrido.

2. En caso de que participen en el tratamiento más de un responsable o encargado, todos los responsables o encargados serán responsables solidarios del importe total de los daños.

3. El responsable o el encargado del tratamiento podrá ser eximido total o parcialmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Artículo 55
Sanciones

Los Estados miembros establecerán las normas sobre las sanciones aplicables a las infracciones de las disposiciones adoptadas con arreglo a la presente Directiva y adoptarán todas las medidas necesarias para garantizar su cumplimiento. Las sanciones establecidas deberán ser efectivas, proporcionadas y disuasorias.

CAPÍTULO IX
ACTOS DELEGADOS Y ACTOS DE EJECUCIÓN

Artículo 56
Ejercicio de la delegación

1. Los poderes para adoptar actos delegados otorgados a la Comisión estarán sujetos a las condiciones establecidas en el presente artículo.

2. La delegación de poderes a que se refiere el artículo 28, apartado 5, se atribuirá a la Comisión por un periodo de tiempo indeterminado a partir de la fecha de entrada en vigor de la presente Directiva.

3. La delegación de poderes a que se refiere el artículo 28, apartado 5, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se

especifiquen. Surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en la fecha posterior que en ella se especifique. No afectará a la validez de los actos delegados que ya estén en vigor.

4. En cuanto la Comisión adopte un acto delegado, lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Todo acto delegado adoptado en virtud del artículo 28, apartado 5, entrará en vigor únicamente en caso de que ni el Parlamento Europeo ni el Consejo hayan manifestado ninguna objeción en un plazo de dos meses a partir de la notificación de dicho acto al Parlamento Europeo y al Consejo, o en caso de que, antes de que expire ese plazo, el Parlamento Europeo y el Consejo hayan informado a la Comisión de que no formularán ninguna objeción. El plazo se podrá prorrogar dos meses a instancias del Parlamento Europeo o del Consejo.

Artículo 57
Procedimiento de Comité

1. La Comisión estará asistida por un Comité. Dicho Comité se entenderá en el sentido del Reglamento (UE) nº 182/2011.

2. Cuando se haga referencia al presente apartado, será de aplicación el artículo 5 del Reglamento (UE) nº 182/2011.

3. Cuando se haga referencia al presente apartado, se aplicará el artículo 8 del Reglamento (UE) nº 182/2011, leído en relación con su artículo 5.

CAPÍTULO X
DISPOSICIONES FINALES

Artículo 58
Derogaciones

1. Queda derogada la Decisión Marco 2008/977/JAI del Consejo.

2. Las referencias a la Decisión Marco derogada a que hace referencia el apartado 1 se entenderán hechas a la presente Directiva.

Artículo 59
Relación con actos de la Unión adoptados anteriormente en el ámbito de la cooperación judicial en materia penal y de la cooperación policial

Las disposiciones específicas relativas a la protección de datos personales en lo que respecta al tratamiento de datos personales por parte de autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales en actos de la Unión adoptados antes de la fecha de adopción de la presente Directiva que regulen el tratamiento de datos personales entre los Estados miembros y el acceso de autoridades designadas de los Estados miembros a los sistemas de información

establecidos con arreglo a lo dispuesto en los Tratados en el ámbito de la presente Directiva no se verán afectadas.

Artículo 60
Relación con acuerdos internacionales celebrados con anterioridad en el ámbito de la cooperación judicial en materia penal y de la cooperación policial

Los acuerdos internacionales celebrados por los Estados miembros con anterioridad a la entrada en vigor de la presente Directiva se modificarán, en caso necesario, en un plazo de cinco años a partir de la entrada en vigor de la presente Directiva.

Artículo 61
Evaluación

1. La Comisión evaluará la aplicación de la presente Directiva.

2. La Comisión revisará en un plazo de tres años después de la entrada en vigor de la presente Directiva otros actos adoptados por la Unión Europea que regulan el tratamiento de datos personales por parte de las autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, en particular los actos adoptados por la Unión a que se refiere el artículo 59, a fin de evaluar la necesidad de aproximarlos a las disposiciones de la presente Directiva, y presentará, en su caso, las propuestas necesarias para modificar dichos actos a fin de garantizar un enfoque coherente de la protección de datos personales en el ámbito de aplicación de la presente Directiva.

3. La Comisión presentará al Parlamento Europeo y al Consejo informes periódicos sobre la evaluación y revisión de la presente Directiva con arreglo a lo dispuesto en el apartado 1. Los primeros informes se presentarán a más tardar cuatro años después de la entrada en vigor de la presente Directiva. Los siguientes informes se presentarán cada cuatro años. La Comisión presentará, si procede, las propuestas oportunas para modificar la presente Directiva y para adaptar otros instrumentos jurídicos. Dicho informe se hará público.

Artículo 62
Implementación

1. Los Estados miembros adoptarán y publicarán, a más tardar el [fecha / dos años después de su entrada en vigor], las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones.

   Aplicarán dichas disposiciones a partir del xx.xx.201x [fecha / dos años después de su entrada en vigor].

   Cuando los Estados miembros adopten dichas disposiciones, estas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación

oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones básicas de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 63
Entrada en vigor y aplicación

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

Artículo 64
Destinatarios

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Bruselas, el 25.1.2012

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*