COMISIÓN EUROPEA

Bruselas, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

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)

(Texto pertinente a efectos del EEE)

{SEC(2012) 72 final}
{SEC(2012) 73 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

La presente exposición de motivos presenta en detalle el nuevo marco jurídico propuesto para la protección de los datos personales en la UE, como se establece en la Comunicación COM (2012) 9 final[1]. El nuevo marco jurídico propuesto 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[2];

La presente exposición de motivos se refiere a la propuesta legislativa de Reglamento general de protección de datos.

La piedra angular de la legislación vigente de la UE en materia de protección de datos, la Directiva 95/46/CE[3], fue adoptada en 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los Estados miembros. Se complementó mediante la Decisión Marco 2008/977/JAI, en su calidad de instrumento general a escala de la Unión para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal[4].

La rápida evolución tecnológica ha supuesto nuevos retos para la protección de los datos personales. Se ha incrementado enormemente la magnitud del intercambio y la recogida de datos. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social.

Generar confianza en el entorno en línea es esencial para el desarrollo económico. La falta de confianza hace que los consumidores vacilen a la hora de adquirir productos en línea y adoptar nuevos servicios, con lo que se corre el riesgo de que se ralentice el desarrollo de usos innovadores de las nuevas tecnologías. La protección de datos personales desempeña, por

---

1 «La protección de la privacidad en un mundo interconectado – Un Marco Europeo de Protección de Datos para el siglo XXI» COM(2012) 9 final.

2 COM(2012) 10 final.

3 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.

4 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, DO L 350 de 30.12.2008, p. 60 («Decisión Marco»).

tanto, una función esencial en la Agenda Digital para Europa[5] y más concretamente en la Estrategia Europa 2020[6].

El artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE), introducido por el Tratado de Lisboa, establece el principio según el cual toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Además, con el artículo 16, apartado 2, del TFUE, el Tratado de Lisboa introdujo una base jurídica específica para la adopción de normas relativas a la protección de datos de carácter personal. El artículo 8 de la Carta de los Derechos Fundamentales de la UE consagra como derecho fundamental la protección de los datos de carácter personal.

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[7]. En su resolución sobre el Programa de Estocolmo, el Parlamento Europeo[8] 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[9], 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.

En su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea»[10], la Comisión concluyó que la UE necesita una política más integradora y coherente en materia del derecho fundamental a la protección de los datos de carácter personal.

Si bien el marco jurídico actual sigue siendo adecuado por lo que respecta a sus objetivos y principios, no ha evitado, sin embargo, la fragmentación en cómo se aplica en la Unión la protección de datos de carácter personal, la inseguridad jurídica y la percepción generalizada de la opinión pública de que existen riesgos significativos, especialmente por lo que se refiere a la actividad en línea[11]. Ha llegado por ello el momento de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas.

---

5 COM(2010) 245 final.

6 COM(2010) 2020 final.

7 «Programa de Estocolmo — Una Europa abierta y segura que sirva y proteja al ciudadano», DO C 115 de 4.5.2010, p.1.

8 Resolución del Parlamento Europeo sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos − Programa de Estocolmo», adoptada el 25 de noviembre de 2009 (P7_TA(2009)0090).

9 COM(2010) 171 final.

10 COM(2010) 609 final.

11 Eurobarómetro especial (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.

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

Esta iniciativa es el resultado de una amplia consulta de todas las partes interesadas sobre la revisión del actual marco jurídico para la protección de datos de carácter personal, que se prolongó durante más de dos años e incluyó una conferencia de alto nivel celebrada en mayo de 2009[12] y 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[13].

– 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[14].

Asimismo se llevaron a cabo consultas selectivas con actores clave; en junio y julio de 2010 se organizaron actos específicos con las autoridades de los Estados miembros y operadores del sector privado, así como con organizaciones de consumidores y entidades dedicadas a la protección de datos y la intimidad[15]. En noviembre de 2010, la Vicepresidenta de la Comisión Europea Viviane Reding organizó una mesa redonda sobre la reforma de la protección de datos. El 28 de enero de 2011 (Día de la protección de datos), la Comisión Europea y el Consejo de Europa organizaron una conferencia de alto nivel con el fin de debatir cuestiones relacionadas con la reforma del marco jurídico de la UE y con la necesidad de establecer unas normas de protección de datos comunes a escala mundial[16]. Las presidencias húngara y polaca del Consejo acogieron sendas conferencias sobre protección de datos los días 16 y 17 de junio de 2011 y el 21 de septiembre de 2011, respectivamente.

A lo largo de 2011 se celebraron talleres y seminarios consagrados específicamente a temas concretos. En enero, ENISA[17] organizó un taller sobre las notificaciones de la violación de datos en Europa[18]. En febrero, la Comisión organizó un taller con las autoridades de los Estados miembros para debatir sobre cuestiones de protección de datos en el ámbito de la cooperación policial y judicial en materia penal, incluida la ejecución de la Decisión Marco, y la Agencia de los Derechos Fundamentales celebró una reunión consultiva con los distintos actores sobre la «Protección de Datos y la Intimidad». El 13 de julio de 2011 tuvo lugar un debate sobre cuestiones clave de la reforma con las autoridades nacionales de protección de datos. Se consultó a los ciudadanos de la UE mediante un Eurobarómetro realizado en

---

12 http://ec.europa.eu/justice/newsroom/data-protection/events/090519_en.htm.

13 Las respuestas no confidenciales pueden consultarse en el sitio internet de la Comisión: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

14 Las respuestas no confidenciales pueden consultarse en el sitio internet de la Comisión: http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

15 http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm.

16 http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day2011_en.asp.

17 Agencia Europea de Seguridad de las Redes y de la Información, que se ocupa de temas de seguridad relacionados con las redes de comunicación y los sistemas de información.

18 Véase http://www.enisa.europa.eu/act/it/data-breach-notification/.

noviembre-diciembre de 2010[19]. Asimismo se pusieron en marcha algunos estudios[20]. El «Grupo de Trabajo del Artículo 29»[21] emitió diversos dictámenes y realizó aportaciones útiles a la Comisión[22]. El 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[23].

Mediante su Resolución de 6 de julio de 2011 el Parlamento Europeo aprobó un informe que respaldaba el enfoque adoptado por la Comisión de cara a reformar el marco de la protección de datos[24]. En sus conclusiones adoptadas el 24 de febrero de 2011, el Consejo de la Unión Europea manifestó su apoyo en general a la intención de la Comisión de reformar el marco de protección de datos y mostró su acuerdo con muchos elementos de la posición de la Comisión. También el Comité Económico y Social Europeo se mostró a favor del objetivo de la Comisión de garantizar una aplicación más coherente de las normas de la UE en materia de protección de datos[25] en todos los Estados miembros y una revisión adecuada de la Directiva 95/46/CE[26].

Durante las consultas sobre el enfoque global, una gran mayoría de los participantes se mostró de acuerdo en que los principios generales siguen siendo válidos, si bien es necesario adaptar el marco vigente para responder mejor a los retos que plantea el rápido desarrollo de las tecnologías (especialmente en línea) y la globalización creciente, al tiempo que se mantiene la neutralidad tecnológica del marco jurídico. La actual fragmentación de la protección de datos personales en la Unión ha sido blanco de duras críticas, especialmente por parte de los operadores económicos, que solicitaron una mayor seguridad jurídica y la armonización de las normas relativas a la protección de los datos de carácter personal. Se considera que la complejidad de las normas en materia de transferencias internacionales de datos personales constituye un impedimento sustancial a su funcionamiento, ya que se necesita transferir con regularidad datos personales de la UE a otras partes del mundo.

---

19 Eurobarómetro especial (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.

20 Además de *Study on the economic benefits of privacy enhancing technologies* (véase la nota a pie de página n° 2), véase también *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, enero de 2010. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf).

21 El Grupo de Trabajo se creó en 1996 (en virtud del artículo 29 de la Directiva) con carácter consultivo y estaba compuesto por representantes de las autoridades nacionales de control de la protección de datos (ACPD), el Supervisor Europeo de Protección de Datos (SEPD) y la Comisión. Para más información sobre sus actividades, véase http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

22 Véanse, en particular, los siguientes dictámenes: sobre el «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 orientación siguientes: sobre notificaciones, datos sensibles y la aplicación práctica del artículo 28, apartado 6, de la Directiva de protección de datos. Todos pueden consultarse en: http://ec.europa.eu/justice/protección de datos/article-29/documentation/index_en.htm.

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

24 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).

25 SEC (2012) 72.

26 CESE 999/2011.

De conformidad con su política «legislar mejor», la Comisión realizó una evaluación de impacto de distintas posibilidades de actuación. 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 general y coherente que abarque todos los ámbitos de competencia de la Unión, incluida la cooperación policial y judicial en materia penal. Se evaluaron tres opciones de actuación con diferentes grados de intervención: la primera opción consistía en la introducción de mínimas enmiendas legislativas y el uso de comunicaciones interpretativas y medidas de apoyo estratégico, como programas de financiación y herramientas técnicas; la segunda opción abarcaba un paquete de disposiciones legislativas que abordaban cada una de las cuestiones identificadas en el análisis, y la tercera opción era la centralización de la protección de datos a nivel de la UE mediante normas precisas y detalladas para todos los sectores y la creación de una agencia de la UE destinada a la supervisión y ejecución de las disposiciones.

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 observaron impactos en el medio ambiente. El análisis del impacto global condujo al desarrollo de la opción estratégica preferida, que se basa en la segunda opción con algunos elementos de las otras dos y se incorpora en la presente propuesta. Según la evaluación de impacto, su ejecución conllevará, entre otras cosas, mejoras considerables en materia de seguridad jurídica para los responsables del tratamiento de datos y los ciudadanos, la reducción de la carga administrativa, la coherencia en la aplicación de la protección de datos en la Unión, la posibilidad efectiva para las personas físicas de ejercer sus derechos de protección de los datos de carácter personal y la eficiencia de la supervisión y la aplicación de la protección de datos. Por otra parte, se espera que la aplicación de la opción estratégica preferida contribuya al objetivo de la Comisión de simplificar y reducir la carga administrativa y a lograr los objetivos de la Agenda Digital para Europa, el Plan de Acción de Estocolmo y la Estrategia Europa 2020.

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

– 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;

– se añadió una sección sobre la proporcionalidad;

– se verificaron y revisaron en su integridad todos los cálculos y estimaciones relativos a la carga administrativa de la hipótesis de base y de la opción preferida, y se aclaró la relación entre los costes de las notificaciones y los costes totales de fragmentación (incluido el anexo 10);

– se especificó mejor la incidencia en las microempresas, las pequeñas y medianas empresas, especialmente de los delegados de protección de datos y las evaluaciones de impacto de la protección de datos.

Con las propuestas se publica un informe de evaluación de impacto y un resumen.

3. ELEMENTOS JURÍDICOS DE LA PROPUESTA

3.1. Base jurídica

La presente propuesta se basa en el artículo 16 del TFUE, que constituye la nueva base jurídica para la adopción de las normas de protección de datos introducida por el Tratado de Lisboa. Esta disposición permite la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión. También permite la adopción de normas relativas a la libre circulación de datos de carácter personal, incluidos los datos personales tratados por los Estados miembros u operadores privados.

Se considera que un Reglamento es el instrumento jurídico más apropiado para definir el marco de la protección de datos personales en la Unión. La aplicabilidad directa de un reglamento, de conformidad con el artículo 288 del TFUE, reducirá la fragmentación jurídica y ofrecerá una mayor seguridad jurídica merced a la introducción de un conjunto armonizado de normas básicas, la mejora de la protección de los derechos fundamentales de las personas y la contribución al funcionamiento del mercado interior.

La referencia al artículo 114, apartado 1, del TFUE solo es necesaria para modificar la Directiva 2002/58/CE en la medida en que dicha Directiva también establece la protección de los intereses legítimos de los abonados que sean personas jurídicas.

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 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, requiere el mismo nivel de protección de datos en toda la Unión. La ausencia de normas comunes de la UE provocaría el riesgo de que hubiera diferentes niveles de protección en los Estados miembros y restricciones en los flujos transfronterizos de datos personales entre los Estados miembros con distintas normas.

– Los datos personales se transfieren a través de las fronteras nacionales, tanto internas como externas, a ritmos cada vez más rápidos. 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 unidad de aplicación del Derecho de la Unión. Por otra parte, 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.

– Las iniciativas legislativas de la UE propuestas serán 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.

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, en el artículo 16 del TFUE y en el artículo 8 del CEDH. Como subrayó el Tribunal de Justicia de la UE[27], el derecho a la protección de datos de carácter personal no es un derecho absoluto, sino que se ha de considerar en relación con su función en la sociedad[28]. La protección de datos está estrechamente ligada 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 los siguientes: la libertad de expresión (artículo 11 de la Carta); la libertad de empresa (artículo 16); el derecho a la propiedad y especialmente a la protección de la propiedad intelectual (artículo 17, apartado 2); la prohibición de toda 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 menor (artículo 24); el derecho a un alto nivel de protección de la salud humana (artículo 35); el derecho de acceso a los documentos (artículo 42); el derecho a la tutela judicial efectiva y a un juez imparcial (artículo 47).

---

27 Tribunal de Justicia de la UE, sentencia de 9.11.2010 en los asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke y Eifert, Rec. 2010, p. I-0000.

28 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.

3.4. Exposición detallada de la propuesta

3.4.1. CAPÍTULO I - DISPOSICIONES GENERALES

El artículo 1 define el objeto del Reglamento y, como el artículo 1 de la Directiva 95/46/CE, establece los dos objetivos del mismo.

El artículo 2 define el ámbito de aplicación material del Reglamento.

El artículo 3 define el ámbito de aplicación territorial del Reglamento.

El artículo 4 contiene definiciones de los términos utilizados en el Reglamento. Si bien algunas definiciones proceden de la Directiva 95/46/CE, otras se modifican, complementadas con elementos adicionales, o se introducen por vez primera («violación de los datos personales» basada en el artículo 2, letra h), de la Directiva sobre la privacidad y las comunicaciones electrónicas 2002/58/CE[29], modificada por la Directiva 2009/136/CE[30]; «datos genéticos»; «datos biométricos»; «datos relativos a la salud»; «establecimiento principal»; «representante»; «empresa»; «grupo de empresas»; «normas corporativas vinculantes»; «niño», que se basa en la Convención de las Naciones Unidas sobre los Derechos del Niño[31], y «autoridad de control»).

En la definición de consentimiento se añade el criterio «explícito» para evitar un paralelismo con consentimiento «inequívoco» que se preste a confusión y con el fin de dotarse de una definición única y coherente que garantice que el interesado es consciente de que da su consentimiento y a qué lo da.

3.4.2. CAPÍTULO II - PRINCIPIOS

El artículo 5 establece los principios relativos al tratamiento de los datos personales, que corresponden a los establecidos en el artículo 6 de la Directiva 95/46/CE. Se introducen nuevos elementos adicionales como el principio de transparencia, la aclaración del principio de minimización de datos y el establecimiento de una responsabilidad general del responsable del tratamiento de datos.

Basado en el artículo 7 de la Directiva 95/46/CE, el artículo 6 establece los criterios que ha de seguir el tratamiento lícito, que se especifican más en profundidad por lo que respecta al criterio del interés, y la observancia de las obligaciones jurídicas y el interés público.

El artículo 7 aclara las condiciones para que el consentimiento sea válido como fundamento jurídico para el tratamiento lícito.

---

29 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), DO L 201 de 31.07.2002, p. 37.

30 Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores (Texto pertinente a efectos del EEE); DO L 337 de 18.12.2009, p. 11.

31 Adoptada y abierta a la firma, ratificación y adhesión por la Resolución de la Asamblea General de las Naciones Unidas 44/25 de 20 de noviembre de 1989.

El artículo 8 establece nuevas condiciones para la licitud del tratamiento de los datos personales de los niños en relación con los servicios de la sociedad de la información que se les ofrecen directamente.

El artículo 9 establece la 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.

El artículo 10 aclara que el responsable del tratamiento no está obligado a obtener información adicional para identificar al interesado con el único fin de cumplir las disposiciones del presente Reglamento.

3.4.3. CAPÍTULO III - DERECHOS DEL INTERESADO

3.4.3.1. Sección 1 – Transparencia y modalidades

El artículo 11 introduce la obligación para los responsables del tratamiento de ofrecer información transparente y de fácil acceso y comprensión, inspirada especialmente en la Resolución de Madrid relativa a estándares internacionales sobre protección de datos personales y privacidad[32].

El artículo 12 obliga al responsable del tratamiento a arbitrar procedimientos y mecanismos para que puedan ejercerse los derechos de los interesados, incluidos los medios para presentar solicitudes electrónicas, con la obligación de responder a la solicitud del interesado en un plazo determinado, y de motivar las denegaciones.

El artículo 13 establece derechos a favor de los destinatarios, basados en el artículo 12, letra c), de la Directiva 95/46/CE, y ampliados a todos los destinatarios, incluidos los corresponsables y coencargados del tratamiento.

3.4.3.2. Sección 2—Información y acceso a los datos

El artículo 14 profundiza en las obligaciones de información del responsable del tratamiento en relación con el interesado, sobre la base de los artículos 10 y 11 de la Directiva 95/46/CE, y dispone el suministro de información adicional al interesado, incluso sobre el periodo de conservación de los datos, el derecho a presentar una reclamación, en relación con las transferencias internacionales y con la fuente de la que proceden los datos. Asimismo mantiene las posibles excepciones de la Directiva 95/46/CE, es decir, no habrá tal obligación si el registro o la comunicación están expresamente previstos por ley. Ello podría aplicarse, por ejemplo, a los procedimientos tramitados por las autoridades de competencia, las administraciones fiscal o aduanera o los servicios competentes en materia de seguridad social.

Basándose en el artículo 12, letra a), de la Directiva 95/46/CE, el artículo 15 dispone el derecho de acceso del interesado a sus datos personales y añade nuevos elementos, como la obligación de informar a los interesados sobre el periodo de conservación, los derechos de rectificación y supresión y a interponer una reclamación.

---

[32] Adoptada por la Conferencia Internacional de Comisarios de Protección de Datos y de la Intimidad de 5 de noviembre de 2009. Véase también el artículo 13, apartado 3, de la propuesta de Reglamento relativo a una normativa común de compraventa europea (COM (2011) 635 final).

3.4.3.3. Sección 3 – Rectificación y supresión

Basándose en el artículo 12, letra b), de la Directiva 95/46/CE, el artículo 16 establece el derecho del interesado a la rectificación.

El artículo 17 establece el derecho del interesado al olvido y de supresión. Asimismo elabora y especifica el derecho de supresión que se establece en el artículo 12, letra b), de la Directiva 95/46/CE y establece las condiciones del derecho al olvido, incluida la obligación del responsable del tratamiento que haya difundido los datos personales de informar a los terceros sobre la solicitud del interesado de suprimir todos los enlaces a los datos personales, copias o réplicas de los mismos. También integra el derecho a que se restrinja el tratamiento en determinados casos, evitando la ambigüedad del término «bloqueo».

El artículo 18 introduce el derecho del interesado a la portabilidad de los datos, es decir, a transferir datos de un sistema de tratamiento electrónico a otro, sin que se lo impida el responsable del tratamiento. A modo de condición previa y con el fin de seguir mejorando el acceso de las personas físicas a sus datos personales, establece el derecho de obtener del responsable esos datos en un formato electrónico estructurado y de uso habitual.

3.4.3.4. Sección 4 – Derecho de oposición y elaboración de perfiles

El artículo 19 establece el derecho de oposición del interesado. Se basa en el artículo 14 de la Directiva 95/46/CE, con algunas modificaciones, especialmente por lo que respecta a la carga de la prueba y su aplicación a la mercadotecnia directa.

El artículo 20 se refiere al derecho del interesado a no ser objeto de una medida basada en la elaboración de perfiles. Con modificaciones y salvaguardias adicionales, se basa en el artículo 15, apartado 1, de la Directiva 95/46/CE en materia de decisiones individuales automatizadas, y toma en consideración la Recomendación del Consejo de Europa sobre la elaboración de perfiles[33].

3.4.3.5. Sección 5 – Restricciones

El artículo 21 aclara la facultad otorgada a la Unión o a los Estados miembros de mantener o introducir restricciones a los principios establecidos en el artículo 5 y a los derechos de los interesados establecidos en los artículos 11 a 20 y en el artículo 32. Esta disposición se basa en el artículo 13 de la Directiva 95/46/CE y en las obligaciones que emanan de la Carta de los Derechos Fundamentales y el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, interpretados por el Tribunal de Justicia de la Unión Europea y el Tribunal Europeo de Derechos Humanos.

3.4.4. CAPÍTULO IV – RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

3.4.4.1. Sección 1 - Obligaciones generales

El artículo 22 toma en consideración el debate sobre un «principio de responsabilidad» y describe pormenorizadamente la obligación de responsabilidad del responsable del tratamiento a la hora de cumplir el presente Reglamento y de demostrar su observancia,

[33] CM/Rec (2010)13.

incluso mediante la adopción de políticas y mecanismos internos que garanticen dicha conformidad.

El artículo 23 establece las obligaciones del responsable del tratamiento que emanan de los principios de la protección de datos desde el diseño y por defecto.

El artículo 24 relativo a los corresponsables aclara sus responsabilidades por lo que se refiere a su relación interna y en relación con el interesado.

El artículo 25 obliga, en determinadas condiciones, a los responsables no establecidos en la Unión, cuando el Reglamento se aplique a sus actividades de tratamiento, a designar un representante en la Unión.

El artículo 26 aclara la posición y la obligación de los encargados del tratamiento, basándose parcialmente en el artículo 17, apartado 2, de la Directiva 95/46/CE y añadiendo nuevos elementos, incluido que todo encargado que trate datos más allá de las instrucciones del responsable del tratamiento ha de ser considerado corresponsable.

El artículo 27 sobre el tratamiento bajo la autoridad del responsable y el encargado se basa en el artículo 16 de la Directiva 95/46/CE.

Para los responsables y encargados del tratamiento, el artículo 28 introduce la obligación de conservar la documentación relativa a las operaciones de tratamiento que estén bajo su responsabilidad, en lugar de una notificación general a la autoridad de control exigida por el artículo 18, apartado 1, y el artículo 19, de la Directiva 95/46/CE.

El artículo 29 aclara las obligaciones del responsable y el encargado del tratamiento de cooperar con la autoridad de control.

3.4.4.2. Sección 2 – Seguridad de los datos

El artículo 30 obliga al responsable y al encargado del tratamiento a adoptar las medidas oportunas para garantizar la seguridad del tratamiento, basándose en el artículo 17, apartado 1, de la Directiva 95/46/CE, extiende la obligación a los encargados, independientemente del contrato suscrito con el responsable del tratamiento.

Los artículos 31 y 32 introducen la obligación de notificar las violaciones de los datos personales, basándose en la notificación de la violación de los datos personales que figura en el artículo 4, apartado 3, de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas.

3.4.4.3. Sección 3 – Evaluación de impacto de la protección de datos y autorización previa

El artículo 33 introduce la obligación de que los responsables y encargados del tratamiento lleven a cabo una evaluación de impacto de la protección de datos antes de efectuar operaciones de tratamiento arriesgadas.

El artículo 34 se refiere a los casos en que es obligatoria la autorización y consulta de la autoridad de control con anterioridad al tratamiento, sobre la base del concepto de control previo establecido en el artículo 20 de la Directiva 95/46/CE.

3.4.4.4. Sección 4 – Delegado de protección de datos

El artículo 35 introduce la obligatoriedad de contar con un delegado de protección de datos en el sector público y en el sector privado, cuando se trate de grandes empresas o en caso de que las actividades principales del responsable o del encargado del tratamiento consistan en operaciones de tratamiento que exijan un seguimiento periódico y sistemático. Esta disposición se fundamenta en el artículo 18, apartado 2, de la Directiva 95/46/CE, que establecía la posibilidad de que los Estados miembros introdujesen este requisito en lugar de una obligación general de notificación.

El artículo 36 crea la figura del delegado de protección de datos.

El artículo 37 establece las tareas esenciales del delegado de protección de datos.

3.4.4.5. Sección 5 – Códigos de conducta y certificación

El artículo 38 se refiere a los códigos de conducta. A tal efecto, inspirado en el concepto del artículo 27, apartado 1, de la Directiva 95/46/CE, aclara el contenido de los códigos y procedimientos, y faculta a la Comisión para decidir sobre la validez general de los códigos de conducta.

El artículo 39 introduce la posibilidad de establecer mecanismos de certificación y sellos y marcados de protección de datos.

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

El artículo 40 establece, como principio general, que la observancia de las obligaciones que figuran en dicho capítulo es de obligado cumplimiento para toda transferencia de datos de carácter personal a terceros países u organizaciones internacionales, incluidas las transferencias ulteriores.

El artículo 41 fija los criterios, condiciones y procedimientos para la adopción de una decisión relativa a la adecuación del nivel de protección de datos por parte de la Comisión, basada en el artículo 25 de la Directiva 95/46/CE. Entre los criterios que deberán tenerse en cuenta para que la Comisión evalúe si existe o no un nivel adecuado de protección se incluyen expresamente el Estado de Derecho, el recurso jurisdiccional y la supervisión independiente. El artículo confirma ahora explícitamente la posibilidad de que la Comisión evalúe el nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país.

Para las transferencias a terceros países en relación con las cuales la Comisión no haya adoptado ninguna decisión de adecuación, el artículo 42 requiere que se aporten las garantías apropiadas, especialmente cláusulas tipo de protección de datos, normas corporativas vinculantes y cláusulas contractuales. La posibilidad de hacer uso de cláusulas tipo de protección de datos de la Comisión se basa en el artículo 26, apartado 4, de la Directiva 95/46/CE. Como novedad, estas cláusulas tipo de protección de datos también pueden ser adoptadas ahora por una autoridad de control y ser declaradas generalmente válidas por la Comisión. Las normas corporativas vinculantes se mencionan ahora específicamente en el texto jurídico. La opción de las cláusulas contractuales ofrece cierta flexibilidad al responsable o al encargado del tratamiento, aunque está sujeta a la autorización previa por parte de las autoridades de control.

El artículo 43 describe con mayor detalle las condiciones aplicables a las transferencias realizadas en el marco de normas corporativas vinculantes, sobre la base de las prácticas y requisitos actuales de las autoridades de control.

El artículo 44 define y aclara las excepciones a una transferencia de datos sobre la base de las disposiciones en vigor del artículo 26 de la Directiva 95/46/CE. Ello se aplica en particular a las transferencias de datos requeridas y necesarias para la protección de intereses públicos importantes, por ejemplo en caso de transferencias internacionales de datos entre autoridades de competencia, administraciones fiscales o aduaneras, o entre servicios competentes en materia de seguridad social o de gestión de la pesca. Por otra parte, en determinadas circunstancias una transferencia de datos puede estar justificada por un interés legítimo del responsable o del encargado del tratamiento, aunque únicamente después de haber evaluado y documentado las circunstancias de dicha operación de transferencia.

El artículo 45 establece explícitamente mecanismos de cooperación internacional para la protección de los datos de carácter personal entre la Comisión y las autoridades de control de terceros países, especialmente aquellas que se considera que ofrecen un nivel de protección adecuado, teniendo en cuenta la Recomendación de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para la cooperación transfronteriza en la ejecución de leyes que protegen la privacidad, de 12 de junio de 2007.

3.4.6. CAPÍTULO V - AUTORIDADES DE CONTROL INDEPENDIENTES

3.4.6.1. Sección 1 - Independencia

El artículo 46 obliga a los Estados miembros a crear autoridades de control, sobre la base del artículo 28, apartado 1, de la Directiva 95/46/CE, y a ampliar su misión para que cooperen entre sí y con la Comisión.

Inspirado también en el artículo 44 del Reglamento (CE) nº 45/2001[34], el artículo 47 aclara las condiciones para la independencia de las autoridades de control, aplicando la jurisprudencia del Tribunal de Justicia de la Unión Europea[35].

El artículo 48 establece las condiciones generales de los miembros de la autoridad de control, en aplicación de la jurisprudencia pertinente[36] e inspirándose también en el artículo 42, apartados 2 a 6, del Reglamento (CE) nº 45/2001.

El artículo 49 establece las normas relativas a la creación de la autoridad de control, que han de establecer por ley los Estados miembros.

El artículo 50 dispone el deber de secreto profesional de los miembros y el personal de la autoridad de control, con base en el artículo 28, apartado 7, de la Directiva 95/46/CE.

---

34 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 008 de 12.1.2001, p.1.

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

36 Op. cit, nota a pie de página nº 34.

3.4.6.2. Sección 2 – Funciones y poderes

El artículo 51 establece la competencia de las autoridades de control. La norma general, basada en el artículo 28, apartado 6, de la Directiva 95/46/CE (competencia en el territorio de su propio Estado miembro), se complementa con la nueva competencia de autoridad principal en caso de que un responsable o encargado del tratamiento esté establecido en varios Estados miembros, con el fin de velar por una aplicación uniforme («principio de ventanilla única»). 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 52 establece las funciones que ha de desempeñar la autoridad de control, entre las que se incluye conocer e investigar las reclamaciones y fomentar el conocimiento de los ciudadanos en materia de riesgos, normas, garantías y derechos.

El artículo 53 dispone los poderes de la autoridad de control, basado en parte en el artículo 28, apartado 3, de la Directiva 95/46/CE y en el artículo 47 del Reglamento (CE) nº 45/2001, y añadiendo algunos elementos nuevos, incluido el poder de sancionar infracciones administrativas.

Inspirado en el artículo 28, apartado 5, de la Directiva 95/46/CE, el artículo 54 obliga a las autoridades de control a elaborar informes anuales de actividad.

3.4.7. CAPÍTULO VII - COOPERACIÓN Y COHERENCIA

3.4.7.1. Sección 1 - Cooperación

Basado en el artículo 28, apartado 6, segundo párrafo, de la Directiva 95/46/CE, el artículo 55 introduce normas explícitas sobre asistencia recíproca obligatoria, incluidas las consecuencias del incumplimiento de la solicitud de otra autoridad de control.

El artículo 56 introduce normas en materia de operaciones conjuntas, inspirado en el artículo 17 de la Decisión 2008/615/JAI[37] del Consejo, incluido el derecho de las autoridades de control a participar en tales operaciones.

3.4.7.2. Sección 2 – Coherencia

El artículo 57 introduce un mecanismo de coherencia para garantizar la uniforme aplicación en las operaciones de tratamiento de datos que pueden afectar a interesados de varios Estados miembros.

El artículo 58 establece los procedimientos y condiciones para un dictamen del Consejo Europeo de Protección de Datos.

El artículo 59 se refiere a los dictámenes de la Comisión sobre los asuntos tratados en el marco del mecanismo de coherencia, que pueden reforzar el dictamen del Consejo Europeo de Protección de datos o expresar una divergencia con dicho dictamen, y al proyecto de medida

[37] Decisión del Consejo 2008/615/JAI, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DO L 210 de 6.8.2008, p. 1.

de la autoridad de control. Cuando la cuestión haya sido planteada por el Consejo Europeo de Protección de Datos en aplicación del artículo 58, apartado 3, es de esperar que la Comisión ejerza su poder discrecional y emita un dictamen, en caso necesario.

El artículo 60 se refiere a las decisiones de la Comisión que obligan a la autoridad competente a suspender su proyecto de medida cuando sea necesario para garantizar la correcta aplicación del presente Reglamento.

El artículo 61 dispone la posibilidad de adoptar medidas provisionales por un procedimiento de urgencia.

El artículo 62 establece los requisitos para los actos de ejecución de la Comisión en el marco del mecanismo de coherencia.

El artículo 63 establece la obligación de que se ejecuten las medidas de una autoridad de control en todos los Estados miembros interesados, y establece que la aplicación del mecanismo de coherencia es condición previa para la validez jurídica y la ejecución de las respectivas medidas.

3.4.7.3. Sección 3 – Consejo Europeo de Protección de Datos

El artículo 64 instituye el Consejo Europeo de Protección de Datos, compuesto por los directores de las autoridades de control de cada Estado miembro y el Supervisor Europeo de Protección de Datos. El Consejo Europeo de Protección de Datos sustituye al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado con arreglo al artículo 29 de la Directiva 95/46/CE. Se aclara que la Comisión no es miembro del Consejo Europeo de Protección de Datos, aunque tiene derecho a participar en sus actividades y a estar representada en el mismo.

El artículo 65 subraya y aclara la independencia del Consejo Europeo de Protección de Datos.

El artículo 66 describe las tareas del Consejo Europeo de Protección de datos, basado en el artículo 30, apartado 1, de la Directiva 95/46/CE, e incluye elementos adicionales, reflejando el creciente abanico de actividades del Consejo Europeo de Protección de Datos, dentro y fuera de la Unión. Con el fin de poder reaccionar en situaciones urgentes, ofrece a la Comisión la posibilidad de solicitar un dictamen en un determinado plazo.

El artículo 67 obliga al Consejo de Europeo de Protección de Datos a presentar informes anuales de actividad, basándose en el artículo 30, apartado 6, de la Directiva 95/46/CE.

El artículo 68 establece los procedimientos de toma de decisiones del Consejo Europeo de Protección de Datos, incluida la obligación de adoptar su reglamento interno, que debe fijar también las disposiciones de funcionamiento.

El artículo 69 incluye disposiciones sobre el presidente y los vicepresidentes del Consejo Europeo de Protección de Datos.

El artículo 70 establece las tareas del presidente.

El artículo 71 establece que el Supervisor Europeo de Protección de Datos llevará a cabo las tareas de secretaría del Consejo Europeo de Protección de Datos y especifica dichas tareas.

El artículo 72 establece normas en materia de confidencialidad.

3.4.8. CAPÍTULO VIII – RECURSOS JUDICIALES, RESPONSABILIDAD Y SANCIONES

Inspirado en el artículo 28, apartado 4, de la Directiva 95/46/CE, el artículo 73 establece el derecho de cualquier interesado a presentar una reclamación ante una autoridad de control. Asimismo especifica los organismos, organizaciones o asociaciones que pueden presentar una reclamación en nombre del interesado o, en caso de violación de los datos personales, con independencia de la reclamación de un interesado.

El artículo 74 se refiere al derecho de recurso judicial contra una autoridad de control. Se basa en la disposición general del artículo 28, apartado 3, de la Directiva 95/46/CE. Establece específicamente un recurso judicial por el que se obliga a la autoridad de control a actuar a raíz de una reclamación y aclara la competencia de los órganos jurisdiccionales del Estado miembro en que esté establecida la autoridad de control. Asimismo ofrece la posibilidad de que la autoridad de control del Estado miembro en el que resida el interesado, ejercite, en nombre del interesado, una acción ante los órganos jurisdiccionales de otro Estado miembro en el que esté establecida la autoridad de control competente.

El artículo 75 se refiere al derecho a un recurso judicial contra un responsable o encargado del tratamiento, basándose en el artículo 22 de la Directiva 95/46/CE, y ofrece la opción de someterse a la jurisdicción del Estado miembro en el que tenga su residencia el demandado o de aquel en el que resida el interesado. Si un procedimiento sobre el mismo asunto estuviera pendiente en el marco del mecanismo de coherencia, el órgano jurisdiccional podrá suspender su procedimiento, salvo en caso de urgencia.

El artículo 76 establece normas comunes para los procedimientos judiciales, incluidos los derechos de los organismos, organizaciones o asociaciones de representar a los interesados ante los tribunales, el derecho de las autoridades de control a ejercitar acciones legales y de los órganos jurisdiccionales a ser informados sobre los procedimientos paralelos en otro Estado miembro, y pudiendo suspender en tal caso el procedimiento[38]. Los Estados miembros están obligados a garantizar la celeridad de las actuaciones judiciales[39].

El artículo 77 establece el derecho a indemnización y responsabilidad. Se basa en el artículo 23 de la Directiva 95/46/CE, amplía este derecho a los daños y perjuicios causados por los encargados del tratamiento y aclara la responsabilidad de los corresponsables y coencargados del tratamiento.

El artículo 78 obliga a los Estados miembros a establecer normas en materia de sanciones, a sancionar las infracciones del Reglamento, y a garantizar su aplicación.

---

[38] Sobre la base del artículo 5, apartado 1, de la Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales, DO L 328 de 15.12.2009, p. 42, y el artículo 13, apartado 1, del Reglamento (CE) nº 1/2003 del Consejo, de 16 de diciembre de 2002, relativo a la aplicación de las normas sobre competencia previstas en los artículos 81 y 82 del Tratado, DO L 1 de 4.1.2003, p.1.

[39] Sobre la base del artículo 18, apartado 1, de la 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 17.7.2000, p. 1.

El artículo 79 obliga a las autoridades de control a sancionar las infracciones administrativas enumeradas en esta disposición, e imponiendo multas hasta un importe máximo, atendiendo a las circunstancias específicas de cada caso.

3.4.9. CAPÍTULO IX – DISPOSICIONES RELATIVAS A SITUACIONES DE TRATAMIENTO DE DATOS ESPECÍFICAS

El artículo 80 obliga a los Estados miembros a adoptar exenciones y excepciones a las disposiciones específicas del Reglamento cuando resulte necesario para conciliar el derecho a la protección de los datos de carácter personal con el derecho a la libertad de expresión. Se basa en el artículo 9 de la Directiva 95/46/CE, tal como ha sido interpretado por el Tribunal de Justicia de la UE[40].

El artículo 81 obliga a los Estados miembros a establecer salvaguardias específicas para el tratamiento con fines sanitarios, además de las condiciones para categorías especiales de datos.

El artículo 82 faculta a los Estados miembros para adoptar leyes específicas para el tratamiento de datos personales en el contexto del empleo.

El artículo 83 establece condiciones específicas para el tratamiento de datos personales con fines históricos, estadísticos y de investigación científica.

El artículo 84 faculta a los Estados miembros para adoptar normas específicas sobre el acceso de las autoridades de control a los datos de carácter personal y a los locales, en caso de que los responsables del tratamiento estén sujetos a obligaciones de confidencialidad.

Inspirado en el artículo 17 del Tratado de Funcionamiento de la Unión Europea, el artículo 85 autoriza la aplicación permanente de las normas generales vigentes en materia de protección de datos de las iglesias, si se ajustan a lo dispuesto en el presente Reglamento.

3.4.10. CAPÍTULO X – ACTOS DELEGADOS Y ACTOS DE EJECUCIÓN

El artículo 86 contiene las disposiciones tipo para el ejercicio de las delegaciones en consonancia con el artículo 290 del TFUE. Ello permite al legislador delegar en la Comisión el poder de adoptar actos no legislativos de alcance general que completen o modifiquen determinados elementos no esenciales de un acto legislativo (actos cuasi legislativos).

El artículo 87 recoge 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.

3.4.11. CAPÍTULO XI - DISPOSICIONES FINALES

El artículo 88 deroga la Directiva 95/46/CEE.

---

[40] Para la interpretación, véase, por ejemplo, Tribunal de Justicia de la Unión Europea, sentencia de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia (C-73/07, Rec. 2008, p. I-9831).

El artículo 89 aclara la relación con la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas, y la modifica.

El artículo 90 obliga a la Comisión a evaluar el Reglamento y presentar los oportunos informes.

El artículo 91 establece la fecha de entrada en vigor del Reglamento y una fase transitoria en lo que respecta a la fecha de su aplicación.

4. REPERCUSIONES PRESUPUESTARIAS

La incidencia presupuestaria específica de la propuesta atañe a las tareas confiadas al Supervisor Europeo de Protección de Datos, tal y como se especifica en la ficha financiera legislativa que acompaña a la presente propuesta. Estas repercusiones requieren una reprogramación de la rúbrica 5 de las Perspectivas Financieras.

La propuesta no tiene incidencia en los gastos operativos.

La ficha financiera legislativa que acompaña a la presente propuesta de Reglamento abarca la incidencia presupuestaria del propio Reglamento y de la Directiva relativa a la protección de datos policiales y judiciales.

2012/0011 (COD)

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)

(Texto pertinente a efectos del EEE)

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, y su artículo 114, apartado 1,

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Comité Económico y Social Europeo[41],

Previa consulta al Supervisor Europeo de Protección de Datos[42],

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 establecen que toda persona tiene derecho a la protección de los datos de carácter personal 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 en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea la nacionalidad o residencia de las personas físicas, 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 y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de los individuos.

---

41 DO C … de… , p. …

42 DO C … de… , p. …

(3) 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[43] pretende armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros.

(4) La integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos. Se ha incrementado en toda la Unión el intercambio de datos entre los operadores económicos y sociales, públicos y privados. El Derecho de la Unión exige a las autoridades nacionales de los Estados miembros que cooperen e intercambien datos personales a fin de poder desempeñar sus funciones o llevar a cabo tareas en nombre de una autoridad de otro Estado miembro.

(5) 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 tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades. Los individuos difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y requiere que se facilite aún más la libre circulación de datos dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

(6) Estos avances requieren el establecimiento de un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Los individuos deben tener el control de sus propios datos personales y se debe reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

(7) Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido la fragmentación en la manera en que se aplica la protección de los datos en el territorio de la Unión, la inseguridad jurídica y una percepción generalizada entre la opinión pública de que existen riesgos significativos para la protección de las personas relacionados especialmente con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas, en particular, del derecho a la protección de los datos de carácter personal, en lo que respecta al tratamiento que se da a dichos datos en los Estados miembros, pueden impedir la libre circulación de los datos de carácter personal en la Unión. Estas diferencias pueden constituir, por lo tanto, un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan los cometidos que les incumben en virtud del Derecho de la Unión. Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE.

---

[43] DO L 281 de 23.11.1995, p. 31.

(8) Para garantizar un nivel uniforme y elevado de protección de las personas y eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión la aplicación coherente y homogénea de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal.

(9) La protección efectiva de los datos personales en la Unión no solo requiere que se refuercen y detallen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, sino también que se otorguen poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y se impongan sanciones equivalentes a los infractores en los Estados miembros.

(10) El artículo 16, apartado 2, del Tratado encarga al Parlamento Europeo y al Consejo que establezcan las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal y las normas relativas a la libre circulación de dichos datos.

(11) Para garantizar un nivel coherente de protección de las personas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos dentro del mercado interior, es necesario un Reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las micro, pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones protegidos jurídicamente y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva de las autoridades de control de los diferentes Estados miembros. Con objeto de tener en cuenta la situación específica de las micro, pequeñas y medianas empresas, el presente Reglamento incluye una serie de excepciones. Además, se anima a las instituciones y órganos de la Unión, los Estados miembros y sus autoridades de control a tomar en consideración las necesidades específicas de las microempresas, pequeñas y medianas empresas en la aplicación del presente Reglamento. El concepto de microempresas, pequeñas y medianas empresas debe tomarse de la Recomendación 2003/361/CE, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

(12) La protección otorgada por el presente Reglamento se refiere a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de datos personales. Por lo que respecta al tratamiento de datos relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto, nadie puede invocar la protección del presente Reglamento. Ello también es de aplicación cuando el nombre de la persona jurídica incluya los nombres de una o más personas físicas.

(13) 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 del presente Reglamento.

(14) El presente Reglamento no aborda cuestiones en materia de protección de los derechos y las libertades fundamentales o la libre circulación de los datos relativos a las actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión, ni tampoco se refiere al tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, que están sujetos al Reglamento (CE) nº 45/2001[44], o por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

(15) El presente Reglamento no debe aplicarse al tratamiento por una persona física de datos de carácter personal que sean exclusivamente personales o domésticos, como la correspondencia y la llevanza de un repertorio de direcciones, sin ningún interés lucrativo y, por tanto, sin conexión alguna con una actividad profesional o comercial. La exención tampoco debe aplicarse a los responsables o encargados del tratamiento que proporcionen los medios para tratar los datos personales relacionados con tales actividades personales o domésticas.

(16) La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y la libre circulación de estos datos, son objeto de un instrumento jurídico específico a nivel de la Unión. Por lo tanto, el presente Reglamento no debe aplicarse a las actividades de tratamiento destinadas a esos fines. No obstante, los datos sometidos a tratamiento por las autoridades públicas en aplicación del presente Reglamento a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, deben regirse por el instrumento jurídico más específico a nivel de la Unión (Directiva XX/YYY).

(17) El presente Reglamento debe entenderse sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular de las normas en materia de responsabilidad de los prestadores de servicios intermediarios dispuestas en los artículos 12 a 15 de la Directiva citada.

(18) El presente Reglamento permite tener en cuenta el principio de acceso público a los documentos oficiales al aplicar sus disposiciones.

(19) Todo tratamiento de datos personales en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de si el tratamiento tiene lugar en la Unión o no. Por establecimiento se entiende el ejercicio efectivo y real de una actividad mediante una instalación estable. Su forma jurídica, ya sea a través de una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto.

---

[44] DO L 8 de 12.1.2001, p. 1.

(20) Con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento, el tratamiento de datos personales de los interesados que residen en la Unión por un responsable del tratamiento no establecido en la Unión debe someterse a lo dispuesto en el presente Reglamento en caso de que las actividades de tratamiento se refieran a la oferta de bienes o servicios a dichos interesados, o al control de la conducta de dichos interesados.

(21) Para determinar si se puede considerar que una actividad de tratamiento «controla la conducta» de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet con técnicas de tratamiento de datos que consistan en la aplicación de un «perfil» a un individuo con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

(22) Cuando sea de aplicación la legislación nacional de un Estado miembro en virtud del Derecho internacional público, el presente Reglamento debe aplicarse también a todo responsable del tratamiento no establecido en la Unión, como los que se encuentren en una misión diplomática u oficina consular.

(23) Los principios de protección deben aplicarse a toda información relativa a una persona identificada o identificable. Para determinar si una persona 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.

(24) Cuando utilizan servicios en línea, las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como las direcciones de los protocolos de internet o los identificadores de sesión almacenados en *cookies*. Ello puede dejar huellas que, combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas e identificarlas. De ello se deduce que los números de identificación, los datos de localización, los identificadores en línea u otros factores específicos no necesariamente tienen que ser considerados datos de carácter personal en toda circunstancia.

(25) Se debe dar el consentimiento de forma explícita por cualquier medio apropiado que permita la manifestación libre, específica e informada de la voluntad del interesado, ya sea mediante una declaración o una clara acción afirmativa del interesado, que garantice que la persona es consciente de que está dando su consentimiento al tratamiento de datos personales, incluso mediante la selección de una casilla de un sitio web en internet o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo fin o fines. Si el consentimiento del interesado se ha de dar a raíz de una solicitud electrónica, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

(26) 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 identifique de manera unívoca a efectos sanitarios; 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.

(27) El establecimiento principal de un responsable del tratamiento en la Unión debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines, condiciones y medios del tratamiento mediante instalaciones estables. Este criterio no debe depender de si el tratamiento de los datos personales se realiza realmente en dicho lugar. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituyen, en sí mismas, dicho establecimiento principal y no son, por lo tanto, criterios definitorios de un establecimiento principal. El establecimiento principal del encargado del tratamiento debe ser el lugar en que tenga su administración central en la Unión.

(28) Un grupo de empresas debe estar constituido por una empresa que ejerce el control y las empresas controladas, en virtud de lo cual la empresa que ejerce el control debe ser la empresa que pueda ejercer una influencia dominante en las otras empresas, por razones, por ejemplo, de propiedad, participación financiera, las normas que la rigen o el poder de hacer que se cumplan las normas de protección de datos personales.

(29) Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos en relación con el tratamiento de datos personales. Con el fin de determinar cuándo se considera que una persona es un niño, el presente Reglamento debe asumir la definición establecida en la Convención de las Naciones Unidas sobre los derechos del niño.

(30) Todo tratamiento de datos de carácter personal debe efectuarse de forma lícita, justa y transparente en relación con las personas interesadas. En particular, los fines específicos para los que se hayan tratado los datos deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos deben ser adecuados, pertinentes y limitarse al mínimo necesario para los fines para los que se traten. Ello requiere, en particular, garantizar que los datos recogidos no sean excesivos y que se limite a un mínimo estricto el periodo en el que se almacenan. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse por otros medios. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Para garantizar que los datos no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.

(31) Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento de la persona interesada o sobre alguna otra base legítima establecida por ley, ya sea en el presente Reglamento ya sea en otros actos legislativos del Estado miembro o de la Unión referidos en el presente Reglamento.

(32) Cuando el tratamiento se lleve a cabo con el consentimiento del interesado, la carga de demostrar que este ha dado su consentimiento a la operación de tratamiento debe recaer en el responsable del tratamiento. En particular, en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente de que da su consentimiento y en qué medida lo hace.

(33) Con el fin de garantizar el consentimiento libre, debe aclararse que este no constituye un fundamento jurídico válido cuando la persona no goza de verdadera libertad de elección y por tanto no está en condiciones de denegar o retirar su consentimiento sin sufrir perjuicio alguno.

(34) El consentimiento no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal cuando exista un desequilibro claro entre el interesado y el responsable del tratamiento. Así sucede especialmente cuando el primero se encuentra en una situación de dependencia respecto del segundo, por ejemplo, cuando los datos personales de los trabajadores son tratados por el empresario en el contexto laboral. Cuando el responsable del tratamiento sea una autoridad pública, solo habría desequilibrio en las operaciones específicas de tratamiento de datos en las que la autoridad pública puede imponer una obligación en virtud de sus poderes públicos correspondientes, sin que pueda considerarse el consentimiento libremente dado, teniendo en cuenta el interés del interesado.

(35) El tratamiento debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de celebrar un contrato.

(36) Cuando se lleve a cabo en cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o si es necesario para el cumplimiento de una misión llevada a cabo por interés público o en el ejercicio de la autoridad pública, el tratamiento debe tener una base jurídica en el Derecho de la Unión o en la legislación de un Estado miembro que cumpla con los requisitos establecidos en la Carta de los Derechos Fundamentales de la Unión Europea en relación con cualquier limitación de los derechos y libertades. Corresponde también al Derecho de la Unión o a las legislaciones nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público debe ser una administración pública u otra persona de derecho público o privado, como por ejemplo una asociación profesional.

(37) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado.

(38) El interés legítimo de un responsable puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado. Ello necesitaría una evaluación meticulosa, especialmente si el interesado fuera un niño, pues los niños merecen una protección específica. Al interesado le debe asistir el derecho a oponerse de forma gratuita al tratamiento de datos, alegando motivos que tengan que ver con su situación particular. Para garantizar la

transparencia, el responsable del tratamiento debe estar obligado a informar explícitamente al interesado del interés legítimo perseguido y del derecho a oponerse, así como a documentar dicho interés legítimo. Dado que corresponde al legislador establecer por ley la base jurídica para que las autoridades públicas traten datos, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones.

(39) Constituye un interés legítimo del responsable el tratamiento de datos en la medida estrictamente necesaria a efectos de garantizar la seguridad de red e información, a saber, la capacidad de un sistema de red o de información de resistir, en un nivel determinado de confianza, acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, y la seguridad de los servicios afines ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de las autoridades públicas, los equipos de respuesta a emergencias informáticas (CERT), los equipos de respuesta a incidentes de seguridad informática (CSIRT), los proveedores de redes y servicios de comunicaciones electrónicas y los proveedores de tecnologías y servicios de seguridad. Se trataría, por ejemplo, de impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, así como detener ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

(40) El tratamiento de datos personales para otros fines solo debe autorizarse cuando sea compatible con aquellos fines para los que los datos hayan sido inicialmente recogidos, en particular cuando el tratamiento sea necesario para fines de investigación histórica, estadística o científica. Cuando esos otros fines no sean compatibles con el propósito inicial para el que se recopilan los datos, el responsable del tratamiento debe obtener el consentimiento del interesado para estos otros fines o debe basarlo en otro motivo legítimo para el tratamiento lícito, especialmente si así lo establece el Derecho de la Unión o la legislación del Estado miembro que sea de aplicación al responsable del tratamiento. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines.

(41) Los datos de carácter personal que, por su naturaleza, sean especialmente sensibles y vulnerables en relación con los derechos fundamentales o la intimidad merecen una protección específica. Tales datos no deben ser tratados, a menos que el interesado dé su consentimiento expreso. No obstante, se deben establecer de forma explícita excepciones a esta prohibición en relación con necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

(42) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías sensibles de datos, siempre que se haga mediante un acto legislativo y se den las garantías apropiadas, a fin de proteger los datos personales y otros derechos fundamentales, cuando así lo justifiquen razones de interés público, incluidas la sanidad pública, la protección social y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o para fines de investigación histórica, estadística y científica.

(43) Por otra parte, el tratamiento de datos personales por parte de las autoridades públicas para alcanzar los objetivos, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente, se realiza por motivos de interés público.

(44) Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en algunos Estados miembros que los partidos políticos recaben datos sobre la ideología política de los ciudadanos, puede autorizarse el tratamiento de estos datos por motivos importantes de interés público, siempre que se establezcan las garantías apropiadas.

(45) Si los datos sometidos a tratamiento no le permiten identificar a una persona física, el responsable no debe estar obligado a recabar información adicional para identificar al interesado con la única finalidad de cumplir lo dispuesto en el presente Reglamento. En caso de que se solicite el acceso, el responsable del tratamiento debe estar facultado para solicitar al interesado información adicional que le permita localizar los datos de carácter personal que esa persona busca.

(46) El principio de transparencia exige que toda información dirigida al público o al interesado sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Ello es especialmente pertinente cuando, en determinadas situaciones, como la publicidad en línea, la proliferación de agentes y la complejidad tecnológica de la práctica, resulte difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, los datos personales que le conciernen. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte específicamente debe facilitarse en un lenguaje claro y llano que puedan comprender con facilidad.

(47) Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar de forma gratuita, entre otras cosas, el acceso a los datos, su rectificación y supresión, y para ejercer el derecho de oposición. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado en un plazo determinado y, en el supuesto de que no las atienda, a explicar sus motivos.

(48) Los principios de tratamiento leal y transparente exigen 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.

(49) 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 un plazo razonable, dependiendo de las circunstancias del caso. Si los datos pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado cuando se desvelan por primera vez.

(50) Sin embargo, no es necesario imponer dicha obligación cuando el interesado ya disponga de esa información, cuando el registro o la comunicación de los datos estén expresamente establecidos por ley, o cuando facilitar los datos al interesado resulte

imposible o exija esfuerzos desproporcionados. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de investigación histórica, estadística o científica; a este respecto, pueden tomarse en consideración el número de interesados, la antigüedad de los datos, y las posibles medidas compensatorias.

(51) 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, la lógica de los datos que se someten a tratamiento y las consecuencias de dicho tratamiento, al menos cuando se basen en la elaboración de perfiles. Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen los programas informáticos. No obstante, estas consideraciones no deben tener como resultado la denegación de toda la información al interesado.

(52) El responsable del tratamiento debe utilizar todas las medidas razonables para verificar la identidad de los interesados que soliciten acceso, en particular en el contexto de los servicios en línea y los identificadores en línea. Los responsables del tratamiento no deben conservar datos personales con el único propósito de poder responder a posibles solicitudes.

(53) Toda persona debe tener derecho a que se rectifiquen los datos personales que le conciernen y «derecho al olvido», cuando la conservación de tales datos no se ajuste a lo dispuesto en el presente Reglamento. En particular, a los interesados les debe asistir el derecho a que se supriman y no se traten sus datos personales, en caso de que ya no sean necesarios para los fines para los que fueron recogidos o tratados de otro modo, de que los interesados hayan retirado su consentimiento para el tratamiento, de que se opongan al tratamiento de datos personales que les conciernan o de que el tratamiento de sus datos personales no se ajuste de otro modo a lo dispuesto en el presente Reglamento. Este derecho es particularmente pertinente si los interesados hubieran dado su consentimiento siendo niños, cuando no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quisieran suprimir tales datos personales especialmente en Internet. Sin embargo, la posterior conservación de los datos debe autorizarse cuando sea necesario para fines de investigación histórica, estadística y científica, por razones de interés publico en el ámbito de la salud pública, para el ejercicio del derecho a la libertad de expresión, cuando la legislación lo exija, o en caso de que existan motivos para restringir el tratamiento de los datos en vez de proceder a su supresión.

(54) Con el fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión también debe ampliarse de tal forma que los responsables del tratamiento que hayan hecho públicos los datos personales deben estar obligados a informar a los terceros que estén tratando tales datos de que un interesado les solicita que supriman todo enlace a tales datos personales, o las copias o réplicas de los mismos. Para garantizar esta información, el responsable del tratamiento debe tomar todas las medidas razonables, incluidas las de carácter técnico, en relación con los datos cuya publicación sea de su competencia. En relación con la publicación de datos personales por un tercero, el responsable del tratamiento debe ser considerado responsable de la publicación, en caso de que haya autorizado la publicación por parte de dicho tercero.

(55) Para reforzar aún más el control sobre sus propios datos y su derecho de acceso, a los interesados les debe asistir el derecho, cuando los datos personales se sometan a tratamiento por medios electrónicos, en un formato estructurado y de uso habitual, a obtener una copia de los datos que les conciernan, también en formato electrónico de uso habitual. Asimismo se debe autorizar a los interesados a transmitir de una aplicación automatizada, como una red social, a otra aquellos datos que hayan facilitado. Tal debe ser el caso cuando el interesado haya facilitado los datos al sistema automatizado de tratamiento, dando su consentimiento o en cumplimiento de un contrato.

(56) En los casos en que los datos personales puedan ser sometidos a tratamiento de forma lícita para proteger intereses vitales del interesado, o por motivos de interés público, de ejercicio del poder público o de los intereses legítimos del responsable del tratamiento, a cualquier interesado le debe asistir el derecho, sin embargo, de oponerse al tratamiento de cualquier dato que le concierna. En el responsable del tratamiento debe recaer la carga de demostrar que sus intereses legítimos pueden prevalecer sobre los intereses o los derechos y libertades fundamentales del interesado.

(57) Cuando los datos personales se sometan a tratamiento con fines de mercadotecnia directa, al interesado le debe asistir el derecho de oponerse a dicho tratamiento de forma gratuita y de una manera que pueda ser invocada con facilidad y efectividad.

(58) Toda persona física debe tener derecho a no ser objeto de medidas que se basen en la elaboración de perfiles por medio de tratamiento automatizado. Sin embargo, se deben permitir tales medidas cuando se autoricen expresamente por actos legislativos, se lleven a cabo en el marco de la celebración o ejecución de un contrato, o el interesado haya dado su consentimiento. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, incluida la información específica del interesado y el derecho a obtener la intervención humana, y dicha medida no debe referirse a un niño.

(59) En la medida en que en una sociedad democrática sea necesario y proporcionado para salvaguardar la seguridad pública, incluida la protección de la vida humana especialmente en respuesta a catástrofes naturales u ocasionadas por el hombre, la prevención, investigación, y el enjuiciamiento de infracciones penales o de violaciones de normas deontológicas en las profesiones reguladas, otros intereses públicos de la Unión o de un Estado miembro, especialmente un importante interés económico o financiero de la Unión o de un Estado miembro, o la protección del interesado o de los derechos y libertades de otros, el Derecho de la Unión o la legislación de los Estados miembros pueden imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación y supresión o al derecho a la portabilidad de los datos, al derecho a oponerse, a las medidas basadas en la elaboración de perfiles, así como a la comunicación de una violación de datos personales a un interesado y a determinadas obligaciones afines de los responsables del tratamiento. Estas restricciones deben ajustarse a lo dispuesto en la Carta de los Derechos Fundamentales de la Unión Europea y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

(60) 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 y está obligado a demostrar que cada operación de tratamiento cumple lo dispuesto en el presente Reglamento.

(61) 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, tanto en el momento del diseño del tratamiento como del tratamiento propiamente dicho, con el fin de garantizar que se cumpla lo dispuesto en el presente Reglamento. Con objeto de garantizar y demostrar el cumplimiento de lo dispuesto en el presente Reglamento, el responsable debe adoptar las políticas internas y aplicar las medidas adecuadas que cumplan especialmente los principios de protección de datos desde el diseño y por defecto.

(62) La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y del encargado del tratamiento, también en relación con la supervisión de las autoridades de control y las medidas adoptadas por ellas, requiere una atribución clara de las responsabilidades con arreglo al presente Reglamento, 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.

(63) Cuando un responsable no establecido en la Unión esté sometiendo a tratamiento datos personales de interesados que residan en la Unión y sus actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados, o con el control de su conducta, el responsable del tratamiento debe designar a un representante, salvo que el primero esté establecido en un tercer país que garantice un nivel de protección adecuado, o sea una pequeña o mediana empresa o una autoridad u organismo público, o en el caso de que el responsable del tratamiento solo ofrezca bienes o servicios ocasionalmente a tales interesados. El representante debe actuar por cuenta del responsable del tratamiento y a él se puede dirigir cualquier autoridad de control.

(64) Para determinar si un responsable del tratamiento solo ofrece ocasionalmente bienes y servicios a interesados residentes en la Unión, debe comprobarse si de las actividades generales del responsable se desprende que la oferta de bienes y servicios a dichos interesados es accesoria a esas actividades principales.

(65) Para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento deben documentar cada operación de tratamiento. Todos los responsables y encargados del tratamiento están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dicha documentación, de modo que pueda servir para supervisar las operaciones de tratamiento.

(66) Con objeto de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos. Estas medidas deben garantizar un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos y la naturaleza de los datos que deban protegerse. A la hora de establecer normas técnicas y medidas organizativas destinadas a garantizar la seguridad del tratamiento, la Comisión debe fomentar la neutralidad tecnológica, la interoperabilidad y la innovación, y, en su caso, cooperar con terceros países.

(67) Una violación de los datos personales puede causar, si no se toman medidas de manera rápida y adecuada, pérdidas económicas sustanciales y perjuicios sociales al

interesado, incluida la usurpación de su identidad. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación, debe notificarla a la autoridad de control sin retraso injustificado y, cuando sea posible, en el plazo de 24 horas. Si no fuera factible en el plazo de 24 horas, la notificación debe ir acompañada de una explicación de las razones de la demora. Las personas cuyos datos personales 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. La notificación debe describir la naturaleza de la violación de los datos personales y las recomendaciones para que la persona afectada mitigue sus potenciales efectos adversos. Las notificaciones a los interesados deben realizarse tan pronto como sea razonablemente posible, en estrecha cooperación con la autoridad de control y siguiendo sus orientaciones o las ofrecidas por otras autoridades competentes (por ejemplo, los servicios con funciones coercitivas). Así, por ejemplo, para que los interesados tengan la oportunidad de mitigar un riesgo inminente de perjuicio se les tendría que notificar de forma inmediata, mientras que la necesidad de aplicar medidas adecuadas para impedir que se sigan violando datos o se produzcan violaciones similares puede justificar un plazo mayor.

(68) Con el fin de determinar si una violación de datos personales se notifica a la autoridad de control y al interesado sin retraso injustificado, se debe evaluar si el responsable del tratamiento ha aplicado las medidas tecnológicas de protección y organización adecuadas con el fin de saber de forma inmediata si se ha producido una violación de datos personales y de informar sin demora a la autoridad de control y al interesado antes de que se produzca un perjuicio a sus intereses económicos y personales, habida cuenta en particular de la naturaleza y gravedad de la violación de los datos personales y sus consecuencias y efectos adversos para el interesado.

(69) 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 usurpación de identidad u otras formas de uso indebido. Asimismo, estas normas y procedimientos deben tener en cuenta los intereses legítimos de los servicios con funciones coercitivas, en los casos en que una comunicación prematura pudiera obstaculizar innecesariamente la investigación de las circunstancias de la violación.

(70) La Directiva 95/46/CE establecía la obligación general de notificar el tratamiento de datos personales a las autoridades de control. A pesar de que esta obligación implica cargas administrativas y financieras, no contribuyó, sin embargo, en todos los casos a mejorar la protección de los datos personales. Por tanto, se debe eliminar esta obligación de notificación tan indiscriminada y debe ser sustituida por procedimientos y mecanismos eficaces que se centren, en su lugar, en las operaciones de tratamiento que, por su naturaleza, alcance o fines, puedan presentar riesgos específicos a los derechos y libertades de los interesados. En tales casos, antes del tratamiento el responsable o el encargado del mismo deben llevar a cabo una evaluación de impacto de la protección de datos, que debe incluir, en particular, las medidas, las garantías y

los mecanismos previstos para garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento.

(71) Ello debe aplicarse, en particular, a los sistemas de archivo a gran escala de reciente creación, que aspiran a tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados.

(72) Hay circunstancias en las que puede resultar sensato y económico que una evaluación de impacto de la protección de datos abarque a más de un único proyecto, por ejemplo, en caso de que las autoridades u organismos públicos tengan la intención de crear una aplicación o plataforma común de tratamiento o de que varios responsables se planteen introducir una aplicación o un entorno de tratamiento común en un sector o segmento de la industria o para una actividad horizontal de uso generalizado.

(73) Las evaluaciones de impacto de la protección de datos deben ser llevadas a cabo por una autoridad o un organismo públicos si tales evaluaciones aún no se han realizado en el contexto de la adopción de la legislación nacional en la que se basa la realización de las tareas de la autoridad o el organismo públicos y que regula la operación o el conjunto de operaciones de tratamiento en cuestión.

(74) Cuando una evaluación de impacto de la protección de datos indique que las operaciones de tratamiento presentan un alto grado de riesgos específicos para los derechos y libertades de los interesados, como el de privar a dichas personas de un derecho, o por la utilización de nuevas tecnologías específicas, la autoridad de control debe ser consultada antes del comienzo de las operaciones en relación con el tratamiento de un riesgo que podría no estar en conformidad con el presente Reglamento, y formular propuestas para corregir esta situación. Dicha consulta también debe realizarse en el curso de la elaboración de una medida por el Parlamento nacional o de una iniciativa basada en dicha medida legislativa que defina la naturaleza del tratamiento y precise las garantías apropiadas.

(75) Si el tratamiento se efectúa en el sector público o en el caso de que, en el sector privado, el tratamiento lo realice una gran empresa, o si sus actividades esenciales, con independencia del tamaño de la empresa, implican operaciones de tratamiento que exijan un seguimiento periódico y sistemático, una persona debe ayudar al responsable o encargado del tratamiento a supervisar la observancia interna del presente Reglamento. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y tareas con independencia.

(76) Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables del tratamiento a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores.

(77) A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación, sellos y marcas de protección de datos, que permitan a los interesados evaluar más rápidamente el nivel de protección de datos de los productos y servicios correspondientes.

(78) Los flujos transfronterizos de datos personales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes con respecto a la protección de los datos de carácter personal. Sin embargo, cuando los datos personales se transfieran de la Unión a terceros países o a organizaciones internacionales, no debe verse menoscabado el nivel de protección de las personas garantizado en la Unión por el presente Reglamento. En cualquier caso, las transferencias hacia terceros países solo pueden llevarse a cabo en conformidad plena con el presente Reglamento.

(79) El presente Reglamento se entiende sin perjuicio de los acuerdos internacionales celebrados entre la Unión y terceros países que regulen la transferencia de datos personales, incluidas las oportunas garantías para los interesados.

(80) 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.

(81) En consonancia con los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos, la Comisión, en su evaluación del tercer país, tiene en cuenta en qué medida este último respeta el Estado de Derecho, el acceso a la justicia, así como las normas y principios relativos a los derechos humanos.

(82) La Comisión también puede reconocer que un tercer país, un territorio o sector del tratamiento en un tercer país, o una organización internacional no ofrece un nivel de protección de datos adecuado. En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país. En ese caso, se debe disponer que se celebren consultas entre la Comisión y dichos terceros países u organizaciones internacionales.

(83) En ausencia de una decisión por la que se constata el carácter adecuado de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante las garantías apropiadas para el interesado. Tales garantías apropiadas pueden consistir en hacer uso de normas corporativas vinculantes, cláusulas tipo de protección de datos adoptadas por la Comisión, cláusulas tipo de protección de datos adoptadas por una autoridad de control o cláusulas contractuales autorizadas por una autoridad de control u otras medidas adecuadas y proporcionadas que se justifiquen a la luz de todas las circunstancias que rodean la operación de transferencia de datos o las operaciones de transferencia de conjuntos de datos y siempre que las autorice una autoridad de control.

(84) La posibilidad de que el responsable o el encargado del tratamiento utilicen cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe impedir que los responsables o encargados del tratamiento incluyan las cláusulas tipo de protección de datos en un contrato más amplio o añadan otras cláusulas, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control o perjudiquen a los derechos o las libertades fundamentales de los interesados.

(85) Todo grupo de sociedades debe poder hacer uso de normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo de empresas, siempre que tales normas corporativas incluyan principios esenciales y derechos aplicables con el fin de asegurar las garantías apropiadas para las transferencias o categorías de transferencias de datos de carácter personal.

(86) Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, cuando el interesado haya dado su consentimiento, la transferencia sea necesaria en relación con un contrato o una reclamación legal, así lo requieran motivos importantes de interés público establecidos por la legislación del Estado miembro o de la Unión, o cuando la transferencia se haga a partir de un registro establecido por ley y se destine a ser consultada por el público o personas con un interés legítimo. En este último caso la transferencia no debe afectar a la totalidad de los datos o de las categorías de datos incluidos en el registro y, cuando el registro esté destinado a ser consultado por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de dichas personas o si estas van a ser las destinatarias.

(87) Estas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias para la protección de motivos importantes de interés público, por ejemplo en caso de transferencias internacionales de datos entre autoridades de competencia, administraciones fiscales o aduaneras, autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social, o a las autoridades competentes para la prevención, investigación, detección y enjuiciamiento de las infracciones penales.

(88) Las transferencias que no puedan considerarse frecuentes o masivas también podrían llevarse a cabo a los fines de satisfacer los intereses legítimos perseguidos por el responsable o el encargado del tratamiento, cuando estos hayan evaluado todas las circunstancias que concurran en la transferencia de datos. A efectos del tratamiento con fines de investigación histórica, estadística y científica, se debe tener en cuenta la confianza legítima de la sociedad en un aumento del conocimiento.

(89) En cualquier caso, cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de protección de los datos en un tercer país, el responsable o el encargado del tratamiento deben arbitrar soluciones que garanticen a los interesados que seguirán beneficiándose de los derechos fundamentales y garantías en lo que se refiere al tratamiento de sus datos en la Unión, una vez que tales datos hayan sido transferidos.

(90) Algunos terceros países promulgan leyes, reglamentaciones y otros instrumentos legislativos con los que se pretende regular directamente las actividades de tratamiento de datos de las personas físicas y jurídicas sujetas a la jurisdicción de los Estados miembros. La aplicación extraterritorial de estas leyes, reglamentaciones y otros instrumentos legislativos puede violar el Derecho internacional y obstaculizar la consecución de la protección de las personas garantizada en la Unión por el presente Reglamento. Solo deben autorizarse las transferencias a terceros países cuando se cumplan las condiciones del presente Reglamento. Tal puede ser el caso, entre otros, cuando la comunicación sea necesaria por una razón importante de interés público reconocida en el Derecho de la Unión o en la legislación de un Estado miembro a la que esté sujeto el responsable del tratamiento. Las condiciones en las que existe una

razón importante de interés público deben ser especificadas en detalle por la Comisión en un acto delegado.

(91) 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, en particular con el fin de protegerse contra la utilización ilícita o la comunicación de dicha información. 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, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. Por tanto, es necesario fomentar una cooperación más estrecha entre las autoridades de control de la protección de datos para ayudarles a intercambiar información y llevar a cabo investigaciones con sus homólogos internacionales.

(92) 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. Los Estados miembros pueden crear más de una autoridad de control con objeto de reflejar su estructura constitucional, organizativa y administrativa.

(93) Si un Estado miembro crea varias autoridades de control, debe establecer por ley mecanismos para garantizar la participación efectiva de dichas autoridades de control en el mecanismo de coherencia. Dicho Estado miembro debe, en particular, designar a la autoridad de control que funcione de punto de contacto único para la participación efectiva de dichas autoridades en el mecanismo, con objeto de garantizar una cooperación rápida y flexible con otras autoridades de control, el Consejo Europeo de Protección de Datos y la Comisión.

(94) 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.

(95) Las condiciones generales aplicables a los miembros de la autoridad de control deben establecerse por ley en cada Estado miembro, 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.

(96) Las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas en aplicación del presente Reglamento y contribuir a su implementación 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 y de facilitar la libre circulación de dichos datos personales en el mercado interior. Para ello, las autoridades de control deben cooperar entre sí y con la Comisión.

(97) Cuando el tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado del tratamiento en la Unión tenga lugar en más de un Estado miembro, una única autoridad de control debe ser competente para supervisar las actividades del responsable o del encargado del

tratamiento en la Unión y tomar las decisiones correspondientes, a fin de potenciar una aplicación coherente, proporcionar seguridad jurídica y reducir la carga administrativa que soportan dichos responsables y encargados.

(98) La autoridad competente que constituye esta ventanilla única debe ser la autoridad de control del Estado miembro en que el responsable o el encargado del tratamiento tengan su establecimiento principal.

(99) Aunque el presente Reglamento 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.

(100) Para garantizar la supervisión y ejecución coherentes del presente Reglamento 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. Los poderes de investigación de las autoridades de control por lo que se refiere al acceso a los locales deben ejercerse de conformidad con el Derecho de la Unión y el Derecho nacional. Ello se refiere especialmente al requisito de obtener un mandato judicial previo.

(101) 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.

(102) Entre las actividades de sensibilización destinadas al público que realicen las autoridades de control deben incluirse medidas específicas dirigidas a los responsables y los encargados del tratamiento, incluidas las microempresas, las pequeñas y medianas empresas, y a los interesados.

(103) Las autoridades de control deben ayudarse en el desempeño de sus tareas y facilitarse ayuda mutua, con el fin de garantizar la aplicación y ejecución coherentes del presente Reglamento en el mercado interior.

(104) Cada autoridad de control debe tener derecho a participar en operaciones conjuntas entre autoridades de control. La autoridad de control requerida debe estar obligada a responder a la solicitud en un plazo determinado.

(105) Con objeto de garantizar la aplicación coherente del presente Reglamento en toda la Unión, debe establecerse un mecanismo de coherencia con vistas a la cooperación entre las propias autoridades de control y la Comisión. Este mecanismo debe aplicarse en particular cuando una autoridad de control tenga intención de adoptar una medida por lo que se refiere a las operaciones de tratamiento relativas a la oferta de bienes o

servicios a los interesados en varios Estados miembros, o a la supervisión de tales interesados, o que puedan afectar de manera sustancial a la libre circulación de los datos personales. También debe aplicarse cuando cualquier autoridad de control o la Comisión soliciten que el asunto se trate en el marco del mecanismo de coherencia. Este mecanismo debe entenderse sin perjuicio de cualesquiera medidas que la Comisión pueda adoptar en el ejercicio de sus competencias, con arreglo a los Tratados.

(106) En aplicación del mecanismo de coherencia, el Consejo Europeo de Protección de Datos debe, en un plazo determinado, emitir un dictamen, si así lo decide una mayoría simple de sus miembros o si así lo solicita cualquier autoridad de control o la Comisión.

(107) Con el fin de garantizar el cumplimiento de lo dispuesto en el presente Reglamento, la Comisión puede adoptar un dictamen sobre este asunto, o una decisión en la que inste a la autoridad de control a suspender su proyecto de medida.

(108) Es posible que haya una necesidad urgente de actuar para proteger los intereses de los interesados, en particular cuando exista el riesgo de que pudiera verse considerablemente obstaculizado el disfrute de alguno de sus derechos. Por lo tanto, las autoridades de control deben estar en condiciones de adoptar medidas provisionales con un determinado período de validez a la hora de aplicar el mecanismo de coherencia.

(109) La aplicación de este mecanismo debe ser una condición para la validez jurídica y la ejecución de la correspondiente decisión por parte de una autoridad de control. En otros casos de relevancia transfronteriza, se podría ofrecer asistencia mutua y llevar a cabo investigaciones conjuntas entre las autoridades de control con carácter bilateral o multilateral sin poner en marcha el mecanismo de coherencia.

(110) A escala de la Unión, se debe crear un Consejo Europeo de Protección de Datos que debe sustituir al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por la Directiva 95/46/CE. Debe estar compuesto por los directores de las autoridades de control de los Estados miembros y el Supervisor Europeo de Protección de Datos. La Comisión debe participar en sus actividades. El Consejo Europeo de Protección de Datos debe contribuir a la aplicación coherente del presente Reglamento en toda la Unión, entre otras cosas, asesorando a la Comisión y fomentando la cooperación de las autoridades de control en toda la Unión. El Consejo Europeo de Protección de Datos debe actuar con independencia en el ejercicio de sus funciones.

(111) Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control en cualquier Estado miembro y tener derecho a presentar un recurso judicial si considera que se vulneran sus derechos en el marco del presente Reglamento 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.

(112) 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.

(113) 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.

(114) Para reforzar la protección judicial del interesado en caso de que la autoridad de control competente esté establecida en un Estado miembro distinto de aquel en el que el interesado resida, este puede solicitar a cualquier entidad, organización o asociación destinadas a proteger los derechos e intereses de los interesados en relación con la protección de sus datos que ejercite acciones legales contra dicha autoridad de control en nombre del interesado ante el órgano jurisdiccional competente del otro Estado miembro.

(115) Cuando la autoridad de control competente establecida en otro Estado miembro no actúe o haya adoptado medidas insuficientes en relación con una reclamación, el interesado puede solicitar a la autoridad de control del Estado miembro de su residencia habitual que ejercite acciones legales contra dicha autoridad de control ante el órgano jurisdiccional competente del otro Estado miembro. La autoridad de control requerida puede decidir, bajo control jurisdiccional, si es oportuno atender la solicitud o no.

(116) Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el demandante debe tener la opción de ejercitarlas ante los órganos jurisdiccionales de los Estados miembros en los que los responsables o encargados del tratamiento estén establecidos o donde tenga su residencia el interesado, a menos que los responsables sean autoridades públicas que actúen en el ejercicio del poder público.

(117) Cuando existan indicios de la existencia de procedimientos paralelos que estén pendientes ante los órganos jurisdiccionales de diferentes Estados miembros, dichos órganos jurisdiccionales deben estar obligados a ponerse en contacto entre sí. Los órganos jurisdiccionales deben tener la posibilidad de suspender una causa cuando en otro Estado miembro se esté tramitando un procedimiento paralelo. Los Estados miembros deben garantizar que las acciones legales, para ser eficaces, permitan la rápida adopción de medidas con el fin de corregir o impedir una infracción del presente Reglamento.

(118) 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.

(119) Deben imponerse sanciones a aquellas personas, ya sean de Derecho público o privado, que no cumplan lo dispuesto en el presente Reglamento. Los Estados miembros deben asegurarse de que las sanciones sean efectivas, proporcionadas y disuasorias y deben tomar todas las medidas para su aplicación.

(120) Con el fin de reforzar y armonizar las sanciones administrativas contra las infracciones de las disposiciones del presente Reglamento, cada autoridad de control debe estar facultado para sancionar las infracciones administrativas. El presente Reglamento debe indicar estas infracciones y el límite máximo para las correspondientes multas administrativas que deben fijarse en cada caso concreto, en proporción a la situación específica, teniendo en cuenta, en particular, la naturaleza, la gravedad y la duración de la violación. El mecanismo de coherencia también puede emplearse para cubrir las divergencias en la aplicación de las sanciones administrativas.

(121) El tratamiento de datos personales solo con fines periodísticos, o con fines de expresión artística o literaria, debe disfrutar de una excepción a los requisitos de determinadas disposiciones del presente Reglamento, con el fin de conciliar el derecho a la protección de los datos de carácter personal con el derecho a la libertad de expresión, y, en especial, el derecho de recibir o de comunicar informaciones, como se garantiza especialmente en el artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea. Ello debe aplicarse en particular al tratamiento de los datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias a efectos de equilibrar estos derechos fundamentales. Tales exenciones y excepciones deben ser adoptadas por los Estados miembros basándose en principios generales, los derechos del interesado, el responsable y encargado del tratamiento, la transferencia de datos a terceros países u organizaciones internacionales, las autoridades de control independientes, así como en la cooperación y la coherencia. No obstante, ello no debe llevar a los Estados miembros a establecer exenciones de las demás disposiciones del presente Reglamento. Con objeto de tomar en consideración la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario interpretar en sentido amplio conceptos relativos a dicha libertad, como el periodismo. Por consiguiente, los Estados miembros deben clasificar determinadas actividades como «periodísticas» a efectos de las exenciones y excepciones que se han de establecer al amparo del presente Reglamento si el objeto de dichas actividades es la comunicación al público de información, opiniones o ideas, con independencia del medio que se emplee para difundirlas. No tienen por qué circunscribirse a empresas de comunicación y pueden desarrollarse con o sin ánimo de lucro.

(122) El tratamiento de datos personales relativos a la salud, como categoría especial de datos que merece mayor protección, puede justificarse a menudo por motivos legítimos en beneficio de los ciudadanos y la sociedad en su conjunto, en particular cuando se trate de garantizar la continuidad de la asistencia sanitaria transfronteriza. Por tanto, el presente Reglamento debe establecer unas condiciones armonizadas para el tratamiento de los datos personales relativos a la salud, sujetas a garantías específicas y adecuadas a fin de proteger los derechos fundamentales y los datos personales de las personas físicas. Ello incluye el derecho de las personas físicas a acceder a sus datos personales relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información de este tipo como los diagnósticos, los resultados de exámenes, las evaluaciones de los facultativos y cualesquiera tratamientos o intervenciones practicadas.

(123) El tratamiento de datos personales relativos a la salud puede ser necesario por razones de interés público en los ámbitos de la salud pública, sin el consentimiento del interesado. En ese contexto, «salud pública» debe interpretarse como se definió en el

Reglamento (CE) nº 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo, es decir, todos los elementos relacionados con la salud, a saber, el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos personales relativos a la salud por razones de interés público no debe tener como consecuencia que terceros, como empresarios, aseguradoras y bancos, sometan a tratamiento datos personales.

(124) Los principios generales sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales también deben ser aplicables al ámbito laboral. Por lo tanto, con el fin de regular el tratamiento de los datos personales de los trabajadores, los Estados miembros, dentro de los límites del presente Reglamento, deben estar facultados para adoptar por ley normas específicas para el tratamiento de datos personales en el ámbito laboral.

(125) Para que sea lícito, el tratamiento de datos de carácter personal a efectos de investigación histórica, estadística o científica también debe respetar otras normas pertinentes, como las relativas a los ensayos clínicos.

(126) A efectos del presente Reglamento, la investigación científica debe abarcar la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado, y, además, debe tener en cuenta el objetivo de la Unión, establecido el en artículo 179, apartado 1, del Tratado de Funcionamiento de la Unión Europea, de realizar un espacio europeo de investigación.

(127) Por lo que respecta a los poderes de las autoridades de control para obtener del responsable o del encargado del tratamiento acceso a los datos personales y a sus locales, los Estados miembros pueden adoptar por ley, dentro de los límites fijados por el presente Reglamento, normas específicas con vistas a salvaguardar las obligaciones de secreto profesional u otras equivalentes, en la medida necesaria para conciliar el derecho a la protección de los datos personales con la obligación de secreto profesional.

(128) El presente Reglamento respeta y no prejuzga el estatuto reconocido, en virtud del Derecho interno, a las iglesias y las asociaciones o comunidades religiosas en los Estados miembros, tal como se reconoce en el artículo 17 del Tratado de Funcionamiento de la Unión Europea. Como consecuencia de ello, cuando una iglesia aplique en un Estado miembro, en el momento de entrada en vigor del presente Reglamento, normas generales relativas a la protección de las personas por lo que respecta al tratamiento de datos personales, estas normas en vigor deben seguir aplicándose si se adaptan a lo dispuesto en el presente Reglamento. Estas iglesias y asociaciones religiosas deben estar obligadas a crear una autoridad de control totalmente independiente.

(129) A fin de cumplir los objetivos del presente Reglamento, a saber, proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y garantizar la libre circulación de los datos

personales en la Unión, debe delegarse a la Comisión el poder de adoptar actos de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea. En particular, los actos delegados deben adoptarse en relación con la licitud del tratamiento; la especificación de los criterios y condiciones en relación con el consentimiento de los niños; el tratamiento de categorías especiales de datos; la especificación de los criterios y condiciones para las solicitudes manifiestamente excesivas y los honorarios para el ejercicio de los derechos del interesado; los criterios y requisitos relativos a la información al interesado y en relación con el derecho de acceso; el derecho al olvido y a la supresión; las medidas basadas en la elaboración de perfiles; los criterios y requisitos en relación con la responsabilidad del responsable del tratamiento y la protección de datos desde el diseño y por defecto; un encargado del tratamiento; los criterios y requisitos relativos a la documentación y la seguridad del tratamiento; los criterios y requisitos para determinar la existencia de una violación de los datos personales y su notificación a la autoridad de control, y sobre las circunstancias en que una violación de los datos personales pueda afectar negativamente al interesado; los criterios y condiciones para las operaciones de tratamiento que requieren una evaluación de impacto en relación con la protección de datos; los criterios y requisitos para determinar un alto grado de riesgos específicos que requieren consulta previa; la designación y las tareas del delegado de protección de datos; los códigos de conducta; los criterios y requisitos para los mecanismos de certificación; los criterios y requisitos para las transferencias por medio de normas corporativas vinculantes; las excepciones a las transferencias; las sanciones administrativas; el tratamiento con fines de salud; el tratamiento en el contexto del empleo y el tratamiento con fines de investigación histórica, estadística y científica. Es de especial importancia que la Comisión evacue las consultas apropiadas durante sus trabajos preparatorios, con expertos inclusive. Al preparar y redactar los actos delegados, la Comisión debe garantizar la transmisión simultánea, oportuna y apropiada de los documentos pertinentes al Parlamento Europeo y al Consejo.

(130) Con el fin de garantizar unas condiciones uniformes para la aplicación del presente Reglamento, se deben conferir competencias de ejecución a la Comisión con objeto de especificar: los formularios tipo en relación con el tratamiento de datos personales de los niños; los procedimientos y formularios tipo para ejercer los derechos de los interesados; los formularios normalizados para informar al interesado; los formularios y procedimientos normalizados en relación con el derecho de acceso; el derecho a la portabilidad de los datos; los formularios normalizados en relación con la responsabilidad del responsable del tratamiento por la protección de datos, desde el diseño y por defecto, y la documentación; los requisitos específicos para la seguridad del tratamiento; el formato estándar y los procedimientos para la notificación de una violación de los datos personales a la autoridad de control y la comunicación de una violación de los datos personales al interesado; las normas y procedimientos para la evaluación de impacto relativa a la protección de datos; los formularios y procedimientos de autorización previa y consulta previa; las normas técnicas y mecanismos de certificación; el nivel adecuado de protección que ofrece un tercer país, un territorio, un sector de tratamiento en ese tercer país o una organización internacional; las comunicaciones no autorizadas por el Derecho de la Unión; la asistencia mutua; las operaciones conjuntas; las decisiones en el marco del mecanismo de coherencia. Es preciso que la Comisión ejerza dichas competencias 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[45]. En este contexto, la Comisión debe plantearse la adopción de medidas específicas para las microempresas, las pequeñas y medianas empresas.

(131) El procedimiento de examen debe emplearse para la adopción de formularios tipo en relación con el consentimiento de los niños; procedimientos y formularios tipo para ejercer los derechos de los interesados; formularios normalizados para informar al interesado; formularios y procedimientos normalizados en relación con el derecho de acceso, el derecho a la portabilidad de los datos; formularios normalizados en relación con la responsabilidad del responsable del tratamiento por la protección de datos desde el diseño y por defecto, y la documentación; requisitos específicos para la seguridad del tratamiento; el formato estándar y los procedimientos para la notificación de una violación de los datos personales a la autoridad de control y la comunicación de una violación de los datos personales al interesado; normas y procedimientos para la evaluación de impacto relativa a la protección de datos; formularios y procedimientos de autorización previa y consulta previa; normas técnicas y mecanismos de certificación; el nivel adecuado de protección que ofrece un tercer país, un territorio, un sector de tratamiento en ese tercer país o una organización internacional; las comunicaciones no autorizadas por el Derecho de la Unión; la asistencia mutua; operaciones conjuntas; decisiones adoptadas en virtud del mecanismo de coherencia, dado que dichos actos son de alcance general.

(132) 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, y relacionados con cuestiones comunicadas por las autoridades de control con arreglo al mecanismo de coherencia.

(133) Dado que los objetivos del presente Reglamento, a saber, garantizar un nivel equivalente de protección de las personas y la libre circulación de datos en la Unión Europea, 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, la Unión 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, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(134) La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Sin embargo, deben seguir en vigor las decisiones de la Comisión adoptadas y las autorizaciones dictadas por las autoridades de control sobre la base de la Directiva 95/46/CE.

(135) El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos

---

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

de carácter personal, que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE, incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas. Para aclarar la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia.

(136) Por lo que se refiere a Islandia y Noruega, el presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen, en la medida en que este se aplica al tratamiento de datos personales por parte de autoridades que participan en la aplicación de dicho acervo, 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[46].

(137) Por lo que se refiere a Suiza, el presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen, en la medida en que este se aplica al tratamiento de datos personales por parte de autoridades que participan en la aplicación de dicho acervo, 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[47].

(138) Por lo que se refiere a Liechtenstein, el presente Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen, en la medida en que este se aplica al tratamiento de datos personales por parte de autoridades que participan en la aplicación de dicho acervo, como se establece en el Protocolo entre la 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, sobre la supresión de controles en las fronteras internas y la circulación de personas[48].

(139) Habida cuenta de que, como ha puesto de relieve el Tribunal de Justicia de la Unión Europea, el derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad, el presente Reglamento respeta todos los derechos fundamentales y observa los principios reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea, consagrados en los Tratados, en particular el derecho al respeto de la vida privada y familiar, al derecho a la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, así como la diversidad cultural, religiosa y lingüística.

---

46 DO L 176 de 10.7.1999, p. 36.
47 DO L 53 de 27.2.2008, p. 52.
48 DO L 160 de 18.6.2011, p. 19.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1
Objeto y objetivos

1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Artículo 2
Ámbito de aplicación material

1. El presente Reglamento se aplica 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.

2. El presente Reglamento no se aplica 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;

   c) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del Tratado de la Unión Europea;

   d) por parte de una persona física sin interés lucrativo en el ejercicio de actividades exclusivamente personales o domésticas;

   e) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

3. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular de las normas en materia de responsabilidad de los prestadores de servicios intermediarios establecidas en los artículos 12 a 15 de la Directiva citada.

Artículo 3
Ámbito de aplicación territorial

1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado del tratamiento en la Unión.

2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable del tratamiento no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

   a) la oferta de bienes o servicios a dichos interesados en la Unión; o

   b) el control de su conducta.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable del tratamiento que no esté establecido en la Unión sino en un lugar en que sea de aplicación la legislación nacional de un Estado miembro en virtud del Derecho internacional público.

Artículo 4
Definiciones

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

5) «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros 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;

6) «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;

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

8) «consentimiento del interesado»: toda manifestación de voluntad, libre, específica, informada y explícita, mediante la que el interesado acepta, ya sea mediante una declaración ya sea mediante una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

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) «establecimiento principal»: en lo que se refiere al responsable del tratamiento, el lugar de su establecimiento en la Unión en el que se adopten las decisiones principales en cuanto a los fines, condiciones y medios del tratamiento de datos personales; si no se adopta en la Unión decisión alguna en cuanto a los fines, condiciones y medios del tratamiento de datos personales, el establecimiento principal es el lugar en el que tienen lugar las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del responsable del tratamiento en la Unión. Por lo que respecta al encargado del tratamiento, por «establecimiento principal» se entiende el lugar de su administración central en la Unión;

14) «representante»: toda persona física o jurídica establecida en la Unión que, designada expresamente por el responsable del tratamiento, actúe en lugar del responsable del tratamiento y a la que pueda dirigirse cualquier autoridad de control y otros organismos de la Unión en lugar del responsable del tratamiento, en lo que respecta a las obligaciones de este último en virtud del presente Reglamento;

15) «empresa»: toda entidad dedicada a una actividad económica, independientemente de su forma jurídica, incluidas, en particular, las personas físicas y jurídicas, así como las sociedades o asociaciones que ejerzan regularmente una actividad económica;

16) «grupo de empresas»: un grupo que comprenda una empresa que ejerce el control y las empresas controladas;

17) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro de la Unión para las transferencias o un conjunto de transferencias de datos personales a un responsable o encargado del tratamiento en uno o más países terceros, dentro de un grupo de empresas;

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

19) «autoridad de control»: la autoridad pública establecida por un Estado miembro de acuerdo con el artículo 46.

CAPÍTULO II
PRINCIPIOS

Artículo 5
Principios relativos al tratamiento de datos personales

Los datos personales deberán ser:

a) tratados de manera lícita, leal y transparente en relación con el interesado;

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

c) adecuados, pertinentes y limitados al mínimo necesario en relación a los fines para los que se traten; solo se tratarán si y siempre que estos fines no pudieran alcanzarse mediante el tratamiento de información que no implique datos personales;

d) exactos y se mantendrán actualizados; se habrán de 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 tratan;

e) conservados en una forma que permita identificar al interesado durante un período no superior al necesario para lo fines para los que se someten a tratamiento; los datos personales podrán ser conservados durante períodos más largos, siempre que se traten exclusivamente para fines de investigación histórica, estadística o científica, con arreglo a las normas y condiciones establecidas en el artículo 83 y si se lleva a cabo una revisión periódica para evaluar la necesidad de seguir conservándolos;

f) tratados bajo la responsabilidad del responsable del tratamiento, que, para cada operación de tratamiento, garantizará y demostrará el cumplimiento de las disposiciones del presente Reglamento.

Artículo 6
Licitud del tratamiento de datos

1. El tratamiento de datos personales solo será lícito en la medida en que sea de aplicación alguno de los siguientes supuestos:

   a) el interesado ha dado su consentimiento para el tratamiento de sus datos personales para uno o más fines específicos;

   b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado;

   c) el tratamiento es necesario para el cumplimiento de una obligación jurídica a la que está sujeto el responsable del tratamiento,

   d) el tratamiento es necesario para proteger intereses vitales del interesado;

   e) el tratamiento es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento;

   f) el tratamiento es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección de los datos personales, en particular, cuando el interesado sea un niño. Ello no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. El tratamiento de los datos personales que sea necesario a efectos de investigación histórica, estadística o científica será lícito siempre que se cumplan las condiciones y garantías previstas en el artículo 83.

3. El fundamento jurídico del tratamiento contemplado en el apartado 1, letras c) y e), se habrá de establecer en:

   a) el Derecho de la Unión, o

   b) en la legislación del Estado miembro a la que esté sujeto el responsable del tratamiento.

   La legislación del Estado miembro deberá cumplir un objetivo de interés público o deberá ser necesaria para proteger los derechos y libertades de terceros, respetar la esencia del derecho a la protección de los datos personales y ser proporcional al objetivo legítimo perseguido.

4. Cuando la finalidad del tratamiento posterior no sea compatible con aquella para la que se recogieron los datos personales, el tratamiento deberá tener base jurídica al menos en uno de los fundamentos mencionados en el apartado 1, letras a) a e). Esto se aplicará en especial a cualquier cambio que se introduzca en las condiciones generales de un contrato.

5. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar las condiciones contempladas en el apartado 1, letra f), para diferentes sectores y situaciones de tratamiento de datos, incluido el tratamiento de los datos personales relativos a los niños.

Artículo 7
Condiciones para el consentimiento

1. El responsable del tratamiento asumirá la carga de la prueba de que el interesado ha dado su consentimiento para el tratamiento de sus datos personales para determinados fines.

2. Si el consentimiento del interesado se ha de dar en el contexto de una declaración escrita que también se refiera a otro asunto, el requisito de dar el consentimiento deberá presentarse de tal forma que se distinga de ese otro asunto.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento antes de su retirada.

4. El consentimiento no constituirá una base jurídica válida para el tratamiento cuando exista un desequilibro claro entre la posición del interesado y el responsable del tratamiento.

Artículo 8
Tratamiento de los datos personales relativos a los niños

1. A efectos del presente Reglamento, en relación con la oferta directa de servicios de la sociedad de la información a los niños, el tratamiento de los datos personales relativos a los niños menores de 13 años solo será lícito si el consentimiento ha sido dado o autorizado por el padre o tutor del niño. El responsable del tratamiento hará esfuerzos razonables para obtener un consentimiento verificable, teniendo en cuenta la tecnología disponible.

2. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como son las normas en materia de validez, formación o efectos de los contratos en relación con un niño.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y condiciones aplicables a los métodos de obtención del consentimiento verificable contemplados en el apartado 1. Para ello, la Comisión se planteará la adopción de medidas específicas para las microempresas, las pequeñas y medianas empresas.

4. La Comisión podrá establecer formularios normalizados para los métodos específicos de obtención del consentimiento verificable contemplados en el apartado 1. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

Artículo 9

Tratamiento de categorías especiales de datos personales

1. Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias, la afiliación sindical, así como el tratamiento de los datos genéticos o los datos relativos a la salud, la vida sexual, las condenas penales o medidas de seguridad afines.

2. El apartado 1 no será aplicable si:

   a) el interesado ha dado su consentimiento para el tratamiento de dichos datos personales, sin perjuicio de las condiciones establecidas en los artículos 7 y 8, excepto cuando el Derecho de la Unión o la legislación de los Estados miembros disponga que la prohibición establecida en el apartado 1 no puede ser levantada por el interesado; o

   b) el tratamiento es necesario para cumplir las obligaciones y ejercer los derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que así lo autorice el Derecho de la Unión o la legislación de los Estados miembros que establezca las garantías apropiadas; o

   c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento; o

   d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a sus miembros, a antiguos miembros del organismo o a personas que mantengan contactos regulares con la fundación, la asociación o el organismo en relación con sus fines y siempre que los datos no se comuniquen fuera del organismo sin el consentimiento de los interesados; o

   e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos; o

   f) el tratamiento es necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; o

   g) el tratamiento es necesario para el cumplimiento de una misión de interés público, sobre la base del Derecho de la Unión o la legislación de los Estados miembros, que establecerán las medidas adecuadas para proteger los intereses legítimos del interesado; o

   h) el tratamiento de datos relativos a la salud es necesario a efectos sanitarios y sin perjuicio de las condiciones y garantías contempladas en el artículo 81; o

   i) el tratamiento es necesario con fines de investigación histórica, estadística o científica, sin perjuicio de las condiciones y garantías contempladas en el artículo 83; o

j) el tratamiento de datos relativos a condenas penales o medidas de seguridad afines se lleva a cabo bajo la supervisión de poderes públicos o si el tratamiento es necesario para cumplir una obligación jurídica o reglamentaria a la que esté sujeto el interesado o para desarrollar una tarea llevada a cabo por motivos importantes de interés público y siempre que lo autorice el Derecho de la Unión o la legislación de los Estados miembros que establezca las garantías apropiadas. Solo se llevará un registro completo de condenas penales bajo el control de los poderes públicos.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios, las condiciones y las garantías apropiadas para el tratamiento de las categorías especiales de datos personales contempladas en el apartado 1 y las excepciones establecidas en el apartado 2.

Artículo 10
Tratamiento que no permite identificación

Si los datos sometidos a tratamiento por un responsable no le permiten identificar a una persona física, el responsable no estará obligado a hacerse con información adicional con vistas a identificar al interesado con la única finalidad de cumplir lo dispuesto en el presente Reglamento.

CAPÍTULO III
DERECHOS DEL INTERESADO

SECCIÓN 1
TRANSPARENCIA Y MODALIDADES

Artículo 11
Transparencia de la información y la comunicación

1. El responsable del tratamiento aplicará políticas transparentes y fácilmente accesibles por lo que respecta al tratamiento de datos personales y al ejercicio de los derechos de los interesados.

2. El responsable del tratamiento facilitará al interesado cualquier información y comunicación relativa al tratamiento de datos personales, en forma inteligible, utilizando un lenguaje sencillo, claro y adaptado al interesado, en particular para cualquier información dirigida específicamente a los niños.

Artículo 12
Procedimientos y mecanismos para el ejercicio de los derechos de los interesados

1. El responsable del tratamiento establecerá procedimientos para facilitar la información contemplada en el artículo 14, y para el ejercicio de los derechos de los interesados contemplados en el artículo 13 y en los artículos 15 a 19. El responsable del tratamiento establecerá, en particular, mecanismos para facilitar la solicitud de las acciones contempladas en el artículo 13 y en los artículos 15 a 19. Cuando los datos

personales se sometan a tratamiento de forma automatizada, el responsable también proporcionará medios para que las solicitudes se hagan por vía electrónica.

2. El responsable del tratamiento informará sin demora al interesado y, a más tardar, en el plazo de un mes a partir de la recepción de la solicitud, de si se ha tomado alguna medida con arreglo a lo dispuesto en el artículo 13 y en los artículos 15 a 19 y facilitará la información solicitada. Este plazo podrá prorrogarse un mes, si varios interesados ejercen sus derechos y si su cooperación es necesaria, en una medida razonable, para impedir un esfuerzo innecesario y desproporcionado por parte del responsable del tratamiento. La información se facilitará por escrito. Cuando el interesado presente la solicitud por vía electrónica, la información se facilitará por vía electrónica, a menos que el interesado solicite que se proceda de otro modo.

3. Si el responsable del tratamiento se niega a dar curso a la solicitud del interesado, le informará de las razones de la denegación y de la posibilidad de presentar una reclamación ante la autoridad de control y de recurrir a los tribunales.

4. La información y las medidas adoptadas sobre las solicitudes contempladas en el apartado 1 serán gratuitas. Cuando las solicitudes sean manifiestamente excesivas, especialmente por su carácter repetitivo, el responsable del tratamiento podrá aplicar una tasa por facilitar la información o adoptar la medida solicitada, o estará facultado para no adoptar la medida solicitada. En ese caso, el responsable del tratamiento asumirá la carga de demostrar el carácter manifiestamente excesivo de la solicitud.

5. La Comisión deberá estar facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y condiciones para las solicitudes manifiestamente excesivas y las tasas contempladas en el apartado 4.

6. La Comisión podrá establecer formularios y procedimientos normalizados para la comunicación contemplada en el apartado 2, incluido el formato electrónico. Para ello, la Comisión adoptará las medidas específicas para las microempresas, las pequeñas y medianas empresas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

Artículo 13
Derechos en relación con los destinatarios

El responsable del tratamiento comunicará cualquier rectificación o supresión llevada a cabo con arreglo a los artículos 16 y 17 a cada uno de los destinatarios a los que se hayan comunicado los datos, salvo que ello sea imposible o exija un esfuerzo desproporcionado.

SECCIÓN 2
INFORMACIÓN Y ACCESO A LOS DATOS

Artículo 14
Información al interesado

1. Cuando se recojan datos personales relativos a un interesado, el responsable del tratamiento le facilitará, al menos, la siguiente información:

a) la identidad y los datos de contacto del responsable del tratamiento y, en su caso, del representante del responsable del tratamiento y del delegado de protección de datos;

b) los fines del tratamiento a que se destinan los datos personales, incluidas las cláusulas y condiciones generales del contrato cuando el tratamiento se base en el artículo 6, apartado 1, letra b), y el interés legítimo perseguido por el responsable del tratamiento cuando el tratamiento se base en el artículo 6, apartado 1, letra f);

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

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

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

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

g) cuando proceda, la intención del responsable del tratamiento de efectuar una transferencia a un tercer país u organización internacional, y el nivel de protección ofrecido por dicho tercer país u organización internacional, con referencia a una decisión de adecuación por parte de la Comisión;

h) cualquier otra información que resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado, habida cuenta de las circunstancias específicas en que se recojan 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. Cuando los datos personales no se recojan del interesado, el responsable del tratamiento le comunicará, además de la información contemplada en el apartado 1, de qué fuente proceden los datos personales.

4. El responsable del tratamiento facilitará la información contemplada en los apartados 1, 2 y 3:

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 obtengan o se sometan a tratamiento de otro modo, o, si se prevé una comunicación a otro destinatario, y a más tardar en el momento en que los datos se comuniquen por primera vez.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando:

a) el interesado ya disponga de la información contemplada en los apartados 1, 2 y 3; o

b) los datos no se recojan del interesado y la comunicación de dicha información resulte imposible o implique un esfuerzo desproporcionado; o

c) los datos no se recojan del interesado y el registro o la comunicación de datos estén expresamente prescritos por ley; o

d) los datos no se recojan del interesado y la comunicación de dicha información menoscabe los derechos y libertades de terceros, como se establece en el Derecho de la Unión o en la legislación de los Estados miembros con arreglo al artículo 21.

6. En el caso contemplado en el apartado 5, letra b), el responsable del tratamiento establecerá las medidas apropiadas para proteger los intereses legítimos del interesado.

7. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios aplicables a las categorías de destinatarios contempladas en el apartado 1, letra f); la obligación de informar sobre las posibilidades de acceso contempladas en el apartado 1, letra g); los criterios aplicables a la obtención de información adicional necesaria contemplada en el apartado 1, letra h), para determinados sectores y situaciones; y las condiciones y garantías apropiadas para las excepciones establecidas en el apartado 5, letra b). Para ello, la Comisión adoptará medidas apropiadas para las microempresas, las pequeñas y medianas empresas.

8. La Comisión podrá establecer formularios normalizados para facilitar la información indicada en los apartados 1 a 3, teniendo en cuenta las características y necesidades específicas de los diferentes sectores y situaciones de tratamiento de datos en caso necesario. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

Artículo 15
Derecho de acceso del interesado

1. Los interesados que lo soliciten tendrán derecho a obtener del responsable del tratamiento, en cualquier momento, confirmación de si se están tratando o no datos personales que les 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 van a comunicarse o han sido comunicados 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 o supresión de datos personales relativos al interesado o a oponerse al tratamiento de dichos datos;

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;

h) la importancia y las consecuencias previstas de dicho tratamiento, al menos en el caso de las medidas contempladas en el artículo 20.

2. El interesado tendrá derecho a que el responsable del tratamiento le comunique los datos personales objeto de tratamiento. Cuando el interesado haga la solicitud en formato electrónico, la información se facilitará en ese mismo formato, a menos que el interesado solicite que se proceda de otro modo.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de precisar los criterios y requisitos aplicables a la comunicación al interesado del contenido de los datos personales contemplada en el apartado 1, letra g).

4. La Comisión podrá especificar formularios y procedimientos normalizados para solicitar y dar acceso a la información contemplada en el apartado 1, en particular con miras a la verificación de la identidad del interesado y la comunicación a este de los datos personales, habida cuenta de las necesidades y características específicas de los distintos sectores y situaciones de tratamiento de datos. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

SECCIÓN 3
RECTIFICACIÓN Y SUPRESIÓN

Artículo 16
Derecho de rectificación

El interesado tendrá derecho 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 adicional.

Artículo 17
Derecho al olvido y a la supresión

1. El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión, especialmente en

lo que respecta a los datos personales proporcionados por el interesado siendo niño, cuando concurra alguna de las circunstancias siguientes:

a) los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados;

b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a), o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos;

c) el interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el artículo 19;

d) el tratamiento de datos no es conforme con el presente Reglamento por otros motivos.

2. Cuando el responsable del tratamiento contemplado en el apartado 1 haya hecho públicos los datos personales, adoptará todas las medidas razonables, incluidas medidas técnicas, en lo que respecta a los datos de cuya publicación sea responsable, con miras a informar a los terceros que estén tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. Cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable de esa publicación.

3. El responsable del tratamiento procederá a la supresión sin demora, salvo en la medida en que la conservación de los datos personales sea necesaria:

a) para el ejercicio del derecho a la libertad de expresión de conformidad con lo dispuesto en el artículo 80;

b) por motivos de interés publico en el ámbito de la salud pública de conformidad con lo dispuesto en el artículo 81;

c) con fines de investigación histórica, estadística y científica de conformidad con lo dispuesto en el artículo 83;

d) para el cumplimiento de una obligación legal de conservar los datos personales impuesta por el Derecho de la Unión o por la legislación de un Estado miembro a la que esté sujeto el responsable del tratamiento; las legislaciones de los Estados miembros deberán perseguir un objetivo de interés público, respetar la esencia del derecho a la protección de datos personales y ser proporcionales a la finalidad legítima perseguida;

e) en los casos contemplados en el apartado 4.

4. En lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de datos personales cuando:

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

b) el responsable del tratamiento ya no necesite los datos personales para la realización de su misión, pero estos deban conservarse a efectos probatorios;

c) el tratamiento sea ilícito y el interesado se oponga a su supresión y solicite en su lugar la limitación de su uso;

d) el interesado solicite la transmisión de los datos personales a otro sistema de tratamiento automatizado de conformidad con lo dispuesto en el artículo 18, apartado 2.

5. Con excepción de su conservación, los datos personales contemplados en el apartado 4 solo podrán ser objeto de tratamiento a efectos probatorios, o con el consentimiento del interesado, o con miras a la protección de los derechos de otra persona física o jurídica o en pos de un objetivo de interés público.

6. Cuando el tratamiento de datos personales esté limitado de conformidad con lo dispuesto en el apartado 4, el responsable del tratamiento informará al interesado antes de levantar la limitación al tratamiento.

7. El responsable del tratamiento implementará mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos personales y/o para el examen periódico de la necesidad de conservar los datos.

8. Cuando se hayan suprimido datos, el responsable del tratamiento no someterá dichos datos personales a ninguna otra forma de tratamiento.

9. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar:

a) los criterios y requisitos relativos a la aplicación del apartado 1 en sectores y situaciones específicos de tratamiento de datos;

b) las condiciones para la supresión de enlaces, copias o réplicas de datos personales procedentes de servicios de comunicación accesibles al público a que se refiere el apartado 2;

c) los criterios y condiciones para limitar el tratamiento de datos personales contemplados en el apartado 4.

Artículo 18
Derecho a la portabilidad de los datos

1. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el interesado tendrá derecho a obtener del responsable del tratamiento una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

2. Cuando el interesado haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico

comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

3. La Comisión podrá especificar el formato electrónico contemplado en el apartado 1 y las normas técnicas, modalidades y procedimientos para la transmisión de datos personales de conformidad con lo dispuesto en el apartado 2. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

SECCIÓN 4

DERECHO DE OPOSICIÓN Y ELABORACIÓN DE PERFILES

Artículo 19
Derecho de oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales sean objeto de un tratamiento basado en el artículo 6, apartado 1, letras d), e) y f), salvo que el responsable del tratamiento acredite motivos imperiosos y legítimos para el tratamiento que prevalezcan sobre los intereses o los derechos y libertades fundamentales del interesado.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse, sin que ello le suponga gasto alguno, al tratamiento de sus datos personales destinado a dicha mercadotecnia directa. Este derecho se ofrecerá explícitamente al interesado de manera inteligible y será claramente distinguible de cualquier otra información.

3. Cuando se formule una oposición de conformidad con lo dispuesto en los apartados 1 y 2, el responsable del tratamiento dejará de usar o tratar de cualquier otra forma los datos personales en cuestión.

Artículo 20
Medidas basadas en la elaboración de perfiles

1. Toda persona física tendrá derecho a no ser objeto de una medida que produzca efectos jurídicos que le conciernan o le afecten de manera significativa y que se base únicamente en un tratamiento automatizado destinado a evaluar determinados aspectos personales propios de dicha persona física o a analizar o predecir en particular su rendimiento profesional, su situación económica, su localización, su estado de salud, sus preferencias personales, su fiabilidad o su comportamiento.

2. A reserva de las demás disposiciones del presente Reglamento, una persona solo podrá ser objeto de una medida del tipo contemplado en el apartado 1 si el tratamiento:

   a) se lleva a cabo en el marco de la celebración o la ejecución de un contrato, cuando la solicitud de celebración o ejecución del contrato presentada por el

interesado haya sido satisfecha o se hayan invocado medidas adecuadas para salvaguardar los intereses legítimos del interesado, como el derecho a obtener una intervención humana; o

b) está expresamente autorizado por el Derecho de la Unión o de un Estado miembro que establezca igualmente medidas adecuadas para salvaguardar los intereses legítimos del interesado; o

c) se basa en el consentimiento del interesado, a reserva de las condiciones establecidas en el artículo 7 y de garantías adecuadas.

3. El tratamiento automatizado de datos personales destinado a evaluar determinados aspectos personales propios de una persona física no se basará únicamente en las categorías especiales de datos personales contempladas en el artículo 9.

4. En los casos contemplados en el apartado 2, la información que debe facilitar el responsable del tratamiento en virtud del artículo 14 incluirá información sobre la existencia del tratamiento por una medida del tipo contemplado en el apartado 1 y los efectos previstos de dicho tratamiento en el interesado.

5. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y condiciones aplicables a las medidas adecuadas para salvaguardar los intereses legítimos del interesado contempladas en el apartado 2.

SECCIÓN 5
LIMITACIONES

Artículo 21
Limitaciones

1. El Derecho de la Unión o de un Estado miembro podrá limitar, por medio de medidas legislativas, el alcance de las obligaciones y de los derechos previstos en el artículo 5, letras a) a e), en los artículos 11 a 20 y en el artículo 32, cuando tal limitación constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar:

a) la seguridad pública;

b) la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales;

c) otros intereses públicos de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, especialmente en los ámbitos fiscal, presupuestario y monetario, así como la protección de la estabilidad y la integridad de los mercados;

d) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

e) una función reglamentaria, de inspección o de supervisión relacionada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a), b), c) y d);

f) la protección del interesado o de los derechos y libertades de otras personas.

2. Cualquier medida legislativa contemplada en el apartado 1 contendrá, en particular, disposiciones específicas al menos en lo tocante a los objetivos del tratamiento y a la identificación del responsable del tratamiento.

CAPÍTULO IV

RESPONSABLE DEL TRATAMIENTO Y ENCARGADO DEL TRATAMIENTO

SECCIÓN 1
OBLIGACIONES GENERALES

Artículo 22
Obligaciones del responsable del tratamiento

1. El responsable del tratamiento adoptará políticas e implementará medidas apropiadas para asegurar y poder demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el presente Reglamento.

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 28;

b) la implementación de los requisitos en materia de seguridad de los datos establecidos en el artículo 30;

c) la realización de una evaluación de impacto en relación con la protección de datos con arreglo a lo dispuesto en el artículo 33;

d) el cumplimiento de los requisitos en materia de autorización o consulta previas de la autoridad de control con arreglo a lo dispuesto en el artículo 34, apartados 1 y 2;

e) la designación de un delegado de protección de datos con arreglo a lo dispuesto en el artículo 35, apartado 1.

3. El responsable del tratamiento implementará mecanismos para verificar la eficacia de las medidas contempladas en los apartados 1 y 2. Siempre que no sea desproporcionado, estas verificaciones serán llevadas a cabo por auditores independientes internos o externos.

4. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar cualesquiera otros criterios y

requisitos aplicables a las medidas apropiadas contempladas en el apartado 1, distintas de las ya mencionadas en el apartado 2, las condiciones para los mecanismos de verificación y auditoría contemplados en el apartado 3 y el criterio de proporcionalidad en virtud del apartado 3, y de considerar la adopción de medidas específicas para las microempresas y las pequeñas y medianas empresas.

Artículo 23
Protección de datos desde el diseño y por defecto

1. Habida cuenta de las técnicas existentes y de los costes asociados a su implementación, el responsable del tratamiento implementará, tanto en el momento de la determinación de los medios de tratamiento como en el del tratamiento propiamente dicho, medidas y procedimientos técnicos y organizativos apropiados, de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento 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 cada fin específico del tratamiento y, especialmente, que no se recojan ni conserven más allá del mínimo necesario para esos fines, tanto por lo que respecta a la cantidad de los datos como a la duración de su conservación. En concreto, estos mecanismos garantizarán que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar cualesquiera nuevos criterios y requisitos aplicables a las medidas y mecanismos apropiados contemplados en los apartados 1 y 2, en particular en lo que respecta a los requisitos en materia de protección de datos desde el diseño aplicables en el conjunto de los sectores, productos y servicios.

4. La Comisión podrá definir normas técnicas para los requisitos establecidos en los apartados 1 y 2. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

Artículo 24
Corresponsables del tratamiento

Cuando un responsable del tratamiento determine, conjuntamente con otros, los fines, las condiciones y los medios del tratamiento de datos personales, los corresponsables determinarán, por mutuo acuerdo, cuáles son sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular por lo que hace a los procedimientos y mecanismos para el ejercicio de derechos del interesado.

Artículo 25
Representantes de los responsables del tratamiento no establecidos en la Unión

1. En el caso contemplado en el artículo 3, apartado 2, el responsable del tratamiento designará un representante en la Unión.

2. Esta obligación no será aplicable a:

a) un responsable del tratamiento establecido en un tercer país cuando la Comisión haya decidido que ese tercer país garantiza un nivel de protección adecuado de conformidad con lo dispuesto en el artículo 41; o

b) una empresa que emplee a menos de doscientas cincuenta personas; o

c) una autoridad u organismo públicos; o

d) un responsable del tratamiento que solo ofrezca ocasionalmente bienes o servicios a interesados residentes en la Unión.

3. El representante deberá estar establecido en uno de los Estados miembros en que residan los interesados cuyos datos personales son objeto de tratamiento en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado.

4. La designación de un representante por el responsable del tratamiento se entenderá sin perjuicio de las acciones legales que pudieran emprenderse contra el propio responsable del tratamiento.

Artículo 26
Encargado del tratamiento

1. Cuando una operación de tratamiento vaya a ser llevada a cabo por cuenta de un responsable del tratamiento, este elegirá 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 las disposiciones del presente Reglamento y garantice la protección de los derechos del interesado, en particular en lo que respecta a las medidas de seguridad técnica y organizativas que rigen el tratamiento que vaya a efectuarse, y velará por que se cumplan dichas medidas.

2. La realización del tratamiento por un encargado se regirá por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento y que disponga, en particular, que el encargado del tratamiento:

a) actuará únicamente siguiendo instrucciones del responsable del tratamiento, en particular cuando la transferencia de los datos personales utilizados esté prohibida;

b) empleará únicamente personal que se haya comprometido a respetar la confidencialidad o esté sujeto a una obligación legal de confidencialidad;

c) tomará todas las medidas necesarias de conformidad con lo dispuesto en el artículo 30;

d) solo recurrirá a otro encargado del tratamiento con la autorización previa del responsable del tratamiento;

e) en la medida de lo posible, y teniendo en cuenta la naturaleza del tratamiento, creará, de acuerdo con el responsable del tratamiento, las condiciones técnicas y organizativas necesarias para permitir al responsable del tratamiento cumplir su obligación de dar curso a las solicitudes que le dirijan los interesados en el ejercicio de sus derechos establecidos en el capítulo III;

f) ayudará al responsable del tratamiento a garantizar el cumplimiento de las obligaciones previstas en los artículos 30 a 34;

g) transmitirá todos los resultados al responsable del tratamiento al término de este y se abstendrá de someter los datos personales a otros tratamientos;

h) pondrá a disposición del responsable del tratamiento y de la autoridad de control toda la información necesaria para controlar el cumplimiento de las obligaciones establecidas en el presente artículo.

3. El responsable y el encargado del tratamiento documentarán por escrito las instrucciones del responsable y las obligaciones del encargado contempladas en el apartado 2.

4. 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 24.

5. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos aplicables a las responsabilidades, funciones y tareas de un encargado del tratamiento de conformidad con lo dispuesto en el apartado 1, así como las condiciones que permitan facilitar el tratamiento de datos personales en un grupo de empresas, en particular a efectos de control y presentación de informes.

Artículo 27

Tratamiento bajo la autoridad del responsable y del encargado del tratamiento

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, a menos que esté obligado a hacerlo por el Derecho de la Unión o de un Estado miembro.

Artículo 28

Documentación

1. Cada responsable y cada encargado del tratamiento, así como, en su caso, el representante del responsable, deberán conservar la documentación de todas las operaciones de tratamiento efectuadas 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, y del representante, si lo hubiera;

b) el nombre y los datos de contacto del delegado de protección de datos, si lo hubiera;

c) los fines del tratamiento, en particular los intereses legítimos perseguidos por el responsable del tratamiento, cuando el tratamiento se base en el artículo 6, apartado 1, letra f);

d) una descripción de las categorías de interesados y de las categorías de datos personales que les conciernen;

e) los destinatarios o las categorías de destinatarios de los datos personales, incluidos los responsables del tratamiento a quienes se comuniquen datos personales por el interés legítimo que persiguen;

f) en su caso, 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 y, en el caso de las transferencias contempladas en el artículo 44, apartado 1, letra h), la documentación de garantías apropiadas;

g) una indicación general de los plazos establecidos para la supresión de las diferentes categorías de datos;

h) la descripción de los mecanismos contemplados en el artículo 22, apartado 3.

3. El responsable y el encargado del tratamiento, así como el representante del responsable, si lo hubiera, pondrán la documentación a disposición de la autoridad de control, a solicitud de esta.

4. Las obligaciones contempladas en los apartados 1 y 2 no serán aplicables a los responsables y los encargados del tratamiento siguientes:

a) personas físicas que traten datos personales sin un interés comercial; o

b) empresas u organizaciones que empleen a menos de doscientas cincuenta personas y que traten datos personales solo como actividad accesoria a sus actividades principales.

5. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos aplicables a la documentación a que se refiere el apartado 1, para tener en cuenta, en particular, las obligaciones del responsable y del encargado del tratamiento y, si lo hubiera, del representante del responsable.

6. La Comisión podrá establecer formularios normalizados para la documentación contemplada en el apartado 1. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

Artículo 29
Cooperación con la autoridad de control

1. El responsable y el encargado del tratamiento, así como el representante del responsable, si lo hubiera, cooperarán con la autoridad de control, si así lo solicita esta, en el desempeño de sus funciones, en particular facilitando la información contemplada en el artículo 53, apartado 2, letra a), y el acceso dispuesto en la letra b) de dicho apartado.

2. Cuando la autoridad de control ejerza los poderes que le son conferidos en virtud del artículo 53, apartado 2, el responsable y el encargado del tratamiento responderán a la autoridad de control dentro de un plazo razonable que será fijado por esta. 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.

SECCIÓN 2
SEGURIDAD DE LOS DATOS

Artículo 30
Seguridad del tratamiento

1. 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 personales que deban protegerse, habida cuenta de las técnicas existentes y de los costes asociados a su implementación.

2. A raíz de una evaluación de los riesgos, el responsable y el encargado del tratamiento adoptarán las medidas contempladas en el apartado 1 a fin de proteger los datos personales contra su destrucción accidental o ilícita, o su pérdida accidental, y de impedir cualquier forma de tratamiento ilícito, en particular la comunicación, la difusión o el acceso no autorizados o la alteración de los datos personales.

3. La Comisión estará facultada para adoptar actos delegados de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y condiciones aplicables a las medidas técnicas y organizativas contempladas en los apartados 1 y 2, incluida la determinación de cuáles son las técnicas existentes, para sectores específicos y en situaciones de tratamiento de datos específicas, habida cuenta en particular de la evolución de la tecnología y de las soluciones de privacidad desde el diseño y la protección de datos por defecto, salvo que sea de aplicación el apartado 4.

4. La Comisión podrá adoptar, en su caso, actos de ejecución para especificar los requisitos establecidos en los apartados 1 y 2 en distintas situaciones, en particular a fin de:

   a) impedir cualquier acceso no autorizado a datos personales;

   b) impedir cualquier forma no autorizada de comunicación, lectura, copia, modificación, supresión o cancelación de datos personales;

   c) garantizar la verificación de la legalidad de las operaciones de tratamiento.

Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

Artículo 31

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

1. 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 no se hace en el plazo de veinticuatro horas, la notificación a la autoridad de control irá acompañada de una justificación motivada.

2. Con arreglo a lo dispuesto en el artículo 26, apartado 2, letra f), 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 de que se trate;

   b) comunicar la identidad y los datos de contacto del delegado de protección de datos 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 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. 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 86, 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 87, apartado 2.

Artículo 32

Comunicación de una violación de datos personales al interesado

1. Cuando sea probable que la violación de datos personales afecte negativamente a la protección de los datos personales o a la privacidad del interesado, el responsable del tratamiento, después de haber procedido a la notificación contemplada en el artículo 31, 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 el artículo 31, 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. Sin perjuicio de la obligación del responsable del tratamiento de comunicar al interesado la violación de datos personales, si aquel no hubiera comunicado ya al interesado la violación de datos personales, la autoridad de control, una vez considerados los efectos negativos probables de la violación, podrá exigirle que lo haga.

5. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos en relación con las circunstancias en que es probable que una violación de datos personales afecte negativamente a los datos personales contemplados en el apartado 1.

6. La Comisión podrá determinar el formato de la comunicación al interesado contemplada en el apartado 1 y los procedimientos aplicables a la misma. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

SECCIÓN 3
EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS Y AUTORIZACIÓN PREVIA

Artículo 33

Evaluación de impacto relativa a la protección de datos

1. Cuando las operaciones de tratamiento entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines, el responsable o el encargado del tratamiento que actúe por cuenta del responsable llevarán a cabo una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.

2. Las siguientes operaciones de tratamiento, en particular, entrañan los riesgos específicos contemplados en el apartado 1:

a) la evaluación sistemática y exhaustiva de los aspectos personales propios de una persona física o destinada a analizar o a predecir, en particular, su situación económica, localización, estado de salud, preferencias personales, fiabilidad o comportamiento, que se base en un tratamiento automatizado y sobre la base de la cual se tomen medidas que produzcan efectos jurídicos que atañan o afecten significativamente a dicha persona;

b) el tratamiento a gran escala de información sobre la vida sexual, la salud, la raza y el origen étnico o destinada a la prestación de atención sanitaria, investigaciones epidemiológicas o estudios relativos a enfermedades mentales o infecciosas, cuando los datos sean tratados con el fin de tomar medidas o decisiones sobre personas concretas;

c) el seguimiento de zonas de acceso público, en particular cuando se utilicen dispositivos optoelectrónicos (videovigilancia) a gran escala;

d) el tratamiento de datos personales en ficheros a gran escala relativos a niños, o el tratamiento de datos genéticos o biométricos;

e) otras operaciones de tratamiento para las cuales sea necesaria la consulta de la autoridad de control con arreglo a lo dispuesto en el artículo 34, apartado 2, letra b).

3. La evaluación deberá incluir, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a los riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos personales y a probar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

4. El responsable del tratamiento recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

5. Cuando el responsable del tratamiento sea una autoridad u organismo públicos y cuando el tratamiento se efectúe en cumplimiento de una obligación legal de conformidad con lo dispuesto en el artículo 6, apartado 1, letra c), que establezca normas y procedimientos relativos a las operaciones de tratamiento y regulados por el Derecho de la Unión, los apartados 1 a 4 no serán aplicables, a menos que los Estados miembros consideren necesario proceder a dicha evaluación con anterioridad a las actividades de tratamiento.

6. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y condiciones aplicables a las operaciones de tratamiento que probablemente presenten los riesgos específicos contemplados en los apartados 1 y 2, y los requisitos aplicables a la evaluación contemplada en el apartado 3, incluidas las condiciones de escalabilidad, verificación y auditabilidad. Al adoptar este tipo de actos, la Comisión considerará la adopción de medidas específicas para las microempresas y las pequeñas y medianas empresas.

7. La Comisión podrá especificar normas y procedimientos para la realización, la verificación y la auditoría de la evaluación contemplada en el apartado 3. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

Artículo 34
Autorización y consulta previas

1. El responsable o el encargado del tratamiento, según proceda, deberán obtener una autorización de la autoridad de control antes de proceder al tratamiento de datos personales a fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, sobre todo, de atenuar los riesgos para los interesados cuando un responsable o un encargado adopten cláusulas contractuales como las contempladas en el artículo 42, apartado 2, letra d), o no ofrezcan garantías apropiadas en un instrumento jurídicamente vinculante como el contemplado en el artículo 42, apartado 5, que rija la transferencia de datos personales a un tercer país o una organización internacional.

2. El responsable o el encargado del tratamiento que actúe por cuenta de aquel deberán consultar a la autoridad de control antes de proceder al tratamiento de datos personales a fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, sobre todo, de atenuar los riesgos para los interesados cuando:

   a) una evaluación del impacto en la protección de los datos, tal como dispone el artículo 33, indique que es probable que las operaciones de tratamiento, por su naturaleza, alcance o fines, entrañen un elevado nivel de riesgos específicos; o

   b) la autoridad de control considere necesario proceder a una consulta previa en relación con las operaciones de tratamiento que probablemente entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance y/o fines, y hayan sido especificadas con arreglo al apartado 4.

3. Cuando la autoridad de control considere que el tratamiento previsto no es conforme con lo dispuesto en el presente Reglamento, en particular cuando los riesgos no estén suficientemente identificados o atenuados, prohibirá el tratamiento previsto y presentará propuestas apropiadas para poner remedio a esta falta de conformidad.

4. La autoridad de control establecerá y publicará una lista de las operaciones de tratamiento que deben ser objeto de una consulta previa de conformidad con lo dispuesto en el apartado 2, letra b). La autoridad de control comunicará estas listas al Consejo Europeo de Protección de Datos.

5. Cuando la lista prevista en el apartado 4 incluya actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados en varios Estados miembros o con el control de su comportamiento, o que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión, la autoridad de control aplicará el mecanismo de coherencia contemplado en el artículo 57 antes de adoptar la lista.

6. El responsable o el encargado del tratamiento facilitarán a la autoridad de control la evaluación de impacto relativa a la protección de datos prevista en el artículo 33 y, previa solicitud, cualquier información adicional que permita a la autoridad de control evaluar la conformidad del tratamiento y, en particular, los riesgos para la protección de los datos personales del interesado y las garantías correspondientes.

7. Los Estados miembros consultarán a la autoridad de control en el marco de la elaboración de una medida legislativa antes de su adopción por los parlamentos nacionales o de una medida basada en una medida legislativa que defina la naturaleza del tratamiento, con el fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, en particular, de atenuar los riesgos para los interesados.

8. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos aplicables a la determinación del nivel elevado de riesgo específico contemplado en el apartado 2, letra a).

9. La Comisión podrá establecer formularios y procedimientos normalizados para las autorizaciones y consultas previas contempladas en los apartados 1 y 2, así como formularios y procedimientos normalizados para informar a las autoridades de control con arreglo a lo dispuesto en el apartado 6. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

SECCIÓN 4
DELEGADO DE PROTECCIÓN DE DATOS

Artículo 35
Designación del delegado de protección de datos

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

   a) el tratamiento sea llevado a cabo por una autoridad u organismo públicos; o

   b) el tratamiento sea llevado a cabo por una empresa que emplee a doscientas cincuenta personas o más; o

   c) las actividades principales del responsable o del encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados.

2. En el caso contemplado en el apartado 1, letra b), un grupo de empresas podrá nombrar un delegado de protección de datos único.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo públicos, el delegado de protección de datos podrá ser designado para varias de sus entidades, teniendo en cuenta la estructura organizativa de la autoridad u organismo públicos.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen categorías de responsables o encargados podrán designar un delegado de protección de datos.

5. El responsable o el encargado del tratamiento designarán el delegado de protección de datos 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 37. El nivel de conocimientos especializados requerido se determinará, en particular, en función del tratamiento de datos llevado a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado del tratamiento.

6. El responsable o el encargado del tratamiento velarán por que cualesquiera otras funciones profesionales del delegado de protección de datos sean compatibles con sus tareas y funciones en calidad de delegado de protección de datos y no planteen conflictos de intereses.

7. El responsable o el encargado del tratamiento designarán un delegado de protección de datos para un mandato mínimo de dos años. El delegado de protección de datos podrá ser nombrado para nuevos mandatos. Durante su mandato, el delegado de protección de datos solo podrá ser destituido si deja de cumplir las condiciones requeridas para el ejercicio de sus funciones.

8. El delegado de protección de datos podrá ser empleado por el responsable o el encargado del tratamiento o desempeñar sus tareas sobre la base de un contrato de servicios.

9. El responsable o el encargado del tratamiento comunicarán el nombre y los datos de contacto del delegado de protección de datos a la autoridad de control y al público.

10. Los interesados tendrán derecho a entrar en contacto con el delegado de protección de datos para tratar todas las cuestiones relativas al tratamiento de datos que les conciernan y a solicitar el ejercicio de los derechos que les confiere el presente Reglamento.

11. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos aplicables a las actividades principales del responsable o del encargado del tratamiento contempladas en el apartado 1, letra c), así como los criterios aplicables a las cualidades profesionales del delegado de protección de datos contempladas en el apartado 5.

Artículo 36
Función de delegado de protección de datos

1. 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 el delegado de protección de datos desempeñe sus funciones y tareas con independencia y no reciba ninguna instrucción en lo que respecta al ejercicio de sus funciones. El delegado de protección de datos informará directamente a la dirección del responsable o del encargado del tratamiento.

3. El responsable o el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de sus tareas y facilitarán el personal, los locales, los equipamientos y cualesquiera otros recursos necesarios para el desempeño de las funciones y tareas contempladas en el artículo 37.

Artículo 37
Tareas del delegado de protección de datos

1. 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 en virtud del presente Reglamento y documentar esta actividad y las respuestas recibidas;

   b) supervisar la implementación y aplicación de las políticas del responsable o del encargado del tratamiento en materia de 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 del presente Reglamento, 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 del presente Reglamento;

   d) velar por la conservación de la documentación contemplada en el artículo 28;

   e) supervisar la documentación, notificación y comunicación de las violaciones de datos personales de conformidad con lo dispuesto en los artículos 31 y 32;

   f) supervisar la realización de la evaluación de impacto relativa a la protección de datos por parte del responsable o del encargado del tratamiento y la presentación de solicitudes de autorización o consulta previas, si fueran necesarias de conformidad con lo dispuesto en los artículos 33 y 34;

   g) supervisar la respuesta a las solicitudes de la autoridad de control y, en el marco de las competencias 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 con la autoridad de control, si procede, a iniciativa propia.

2. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos aplicables a las tareas, la certificación, el estatuto, las competencias y los recursos del delegado de protección de datos contemplados en el apartado 1.

SECCIÓN 5
CÓDIGOS DE CONDUCTA Y CERTIFICACIÓN

Artículo 38
Códigos de conducta

1. Los Estados miembros, las autoridades de control y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento de datos, especialmente en lo que respecta a:

   a) el tratamiento equitativo y transparente de los datos;

   b) la recogida de datos;

   c) la información del público y de los interesados;

   d) las solicitudes formuladas por los interesados en el ejercicio de sus derechos;

   e) la información y la protección de los niños;

   f) la transferencia de datos a terceros países u organizaciones internacionales;

   g) los mecanismos para supervisar y garantizar el cumplimiento de las disposiciones del código por parte de los responsables del tratamiento que se hayan adherido a él;

   h) los procedimientos extrajudiciales y otros procedimientos de resolución de litigios que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento de datos personales, sin perjuicio de los derechos de los interesados de conformidad con los artículos 73 y 75.

2. Las asociaciones y otros organismos que representen a categorías de responsables o encargados del tratamiento en un Estado miembro que tengan la intención de elaborar códigos de conducta o de modificar o ampliar códigos de conducta existentes podrán someterlos al dictamen de la autoridad de control en dicho Estado miembro. La autoridad de control podrá emitir un dictamen sobre la conformidad con el presente Reglamento del proyecto de código de conducta o de su modificación. La autoridad de control recabará el parecer de los interesados o de sus representantes sobre estos proyectos.

3. Las asociaciones y otros organismos que representen a categorías de responsables del tratamiento en varios Estados miembros podrán presentar a la Comisión proyectos de códigos de conducta, así como modificaciones o ampliaciones de códigos de conducta existentes.

4. La Comisión podrá adoptar actos de ejecución para decidir que los códigos de conducta y las modificaciones o ampliaciones de códigos de conducta existentes que les sean sometidos con arreglo a lo dispuesto en el apartado 3 tienen validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

5. La Comisión asegurará una publicidad adecuada de los códigos cuya validez general haya sido decidida de conformidad con el apartado 4.

Artículo 39
Certificación

1. Los Estados miembros y la Comisión promoverán, en particular a nivel europeo, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcados de protección de datos que permitan a los interesados evaluar rápidamente el nivel de protección de datos que ofrecen los responsables y los encargados del tratamiento. Los mecanismos de certificación en materia de protección de datos contribuirán a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores y las diferentes operaciones de tratamiento.

2. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos aplicables a los mecanismos de certificación en materia de protección de datos contemplados en el apartado 1, en particular las condiciones de concesión y revocación, así como los requisitos en materia de reconocimiento en la Unión y en terceros países.

3. La Comisión podrá establecer normas técnicas para los mecanismos de certificación y los sellos y marcados de protección de datos, y mecanismos para promover y reconocer los mecanismos de certificación y los sellos y marcados de protección de datos. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

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

Artículo 40
Principio general de las transferencias

Solo podrán realizarse transferencias de datos personales que sean o vayan a ser objeto de tratamiento tras su transferencia a un tercer país o a una organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, en particular en lo tocante a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

Artículo 41

Transferencias con una decisión de adecuación

1. Podrá realizarse una transferencia cuando la Comisión haya decidido que el tercer país, o un territorio o un sector de tratamiento de datos 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. Al evaluar la adecuación del nivel de protección, la Comisión tomará 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 y el Derecho penal, las normas profesionales y 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 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 87, 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 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 eficaces 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. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen contemplado en el artículo 87, 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 87, apartado 3.

6. Cuando la Comisión adopte una decisión de conformidad con lo dispuesto en el apartado 5, estará 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, sin perjuicio de lo dispuesto en los artículos 42 a 44. 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.

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, y de las organizaciones internacionales para los que haya decidido que está o no está garantizado un nivel protección adecuado.

8. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, o del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por la Comisión.

Artículo 42
Transferencias mediante garantías apropiadas

1. Cuando la Comisión no haya adoptado una decisión con arreglo a lo dispuesto en el artículo 41, un responsable o un encargado del tratamiento solo podrán transferir datos personales a un tercer país o una organización internacional si hubieran ofrecido garantías apropiadas en lo que respecta a la protección de datos personales en un instrumento jurídicamente vinculante.

2. Constituirán garantías apropiadas a tenor de lo dispuesto en el apartado 1, en particular:

   a) las normas corporativas vinculantes de conformidad con el artículo 43; o

   b) las cláusulas tipo de protección de datos adoptadas por la Comisión; dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 87, apartado 2; o

   c) las cláusulas tipo de protección de datos adoptadas por una autoridad de control de conformidad con el mecanismo de coherencia contemplado en el artículo 57, cuando la Comisión haya declarado que tienen validez general con arreglo al artículo 62, apartado 1, letra b); o

   d) las cláusulas contractuales entre el responsable o el encargado del tratamiento y el destinatario de los datos autorizadas por una autoridad de control de conformidad con lo dispuesto en el apartado 4.

3. Una transferencia efectuada en virtud de cláusulas tipo de protección de datos o de normas corporativas vinculantes como las contempladas en el apartado 2, letras a), b) o c), no requerirá nuevas autorizaciones.

4. Cuando una transferencia se efectúe en virtud de cláusulas contractuales como las contempladas en la letra d) del apartado 2, el responsable o el encargado del tratamiento deberán haber obtenido de la autoridad de control la autorización previa de las cláusulas contractuales con arreglo a lo dispuesto en el artículo 34, apartado 1. Si la transferencia se refiere a actividades de tratamiento que atañan a interesados en otro u otros Estados miembros o que afecten sustancialmente a la libre circulación de datos personales dentro de la Unión, la autoridad de control aplicará el mecanismo de coherencia contemplado en el artículo 57.

5. Cuando las garantías apropiadas con respecto a la protección de datos personales no se proporcionen en un instrumento jurídicamente vinculante, el responsable o el encargado del tratamiento deberán obtener la autorización previa de la transferencia o serie de transferencias, o de las disposiciones que se vayan a insertar en el acuerdo administrativo que constituye la base de dicha transferencia. Una autorización de esta índole concedida por la autoridad de control deberá ser conforme con lo dispuesto en el artículo 34, apartado 1. Si la transferencia se refiere a actividades de tratamiento que atañan a interesados en otro u otros Estados miembros o que afecten sustancialmente a la libre circulación de datos personales dentro de la Unión, la autoridad de control aplicará el mecanismo de coherencia contemplado en el artículo 57. Las autorizaciones otorgadas por una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas por dicha autoridad de control.

Artículo 43

Transferencias mediante normas corporativas vinculantes

1. Una autoridad de control aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 58, siempre que estas:

   a) sean jurídicamente vinculantes y se apliquen a todos los miembros del grupo de empresas del responsable o del encargado del tratamiento, incluidos sus empleados, que asegurarán su cumplimiento;

   b) confieran expresamente a los interesados derechos exigibles;

   c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes especificarán, como mínimo:

   a) la estructura y los datos de contacto del grupo de empresas y de sus miembros;

   b) las transferencias o serie de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

   c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

   d) los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la calidad de los datos, la base jurídica del tratamiento, el tratamiento de datos personales sensibles, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos en materia

de transferencias ulteriores a organizaciones que no estén vinculadas por esas políticas;

e) los derechos de los interesados y los medios para ejercerlos, en particular el derecho a no ser objeto de una medida basada en la elaboración de perfiles de conformidad con lo dispuesto en el artículo 20, el derecho a presentar una reclamación ante la autoridad de control competente y ante los órganos jurisdiccionales competentes de los Estados miembros de conformidad con lo dispuesto en el artículo 75, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro del grupo de empresas no establecido en la Unión; el responsable o el encargado del tratamiento solo podrán ser exonerados de esta responsabilidad, total o parcialmente, si prueban que el acto que originó el daño no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f), de conformidad con lo dispuesto en el artículo 11;

h) las tareas del delegado de protección de datos designado de conformidad con lo dispuesto en el artículo 35, en particular la supervisión, dentro del grupo de empresas, del cumplimiento de las normas corporativas vinculantes, así como la supervisión de la formación y de la tramitación de las reclamaciones;

i) los mecanismos establecidos dentro del grupo de empresas para garantizar que se verifica el cumplimiento de las normas corporativas vinculantes;

j) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las políticas y para notificar esas modificaciones a la autoridad de control;

k) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de todos los miembros del grupo de empresas, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra i).

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos aplicables a las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo, en particular en lo que respecta a los criterios aplicables a su aprobación, la aplicación de las letras b), d), e) y f) del apartado 2 a las normas corporativas vinculantes a las que se hayan adherido los encargados del tratamiento, y otros requisitos necesarios para garantizar la protección de los datos personales de los interesados afectados.

4. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información por vía electrónica entre los responsables del tratamiento, los encargados del tratamiento y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

Artículo 44
Excepciones

1. En ausencia de una decisión de adecuación de conformidad con lo dispuesto en el artículo 41 o de garantías apropiadas de conformidad con lo dispuesto en el artículo 42, solo podrá procederse a una transferencia o una serie de transferencias de datos personales a un tercer país o una organización internacional cuando:

a) el interesado haya dado su consentimiento a la transferencia propuesta, tras haber sido informado de los riesgos que entraña debido a la ausencia de una decisión de adecuación y de garantías apropiadas; o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la implementación de medidas precontractuales adoptadas a solicitud del interesado; o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica; o

d) la transferencia sea necesaria por motivos importantes de interés público; o

e) la transferencia sea necesaria para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial; o

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otra persona, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; o

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de un Estado miembro, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de un Estado miembro para la consulta; o

h) la transferencia sea necesaria para la satisfacción de los intereses legítimos del responsable o del encargado del tratamiento, que no puedan ser calificados de frecuentes ni de masivos, y el responsable o el encargado hayan evaluado todas las circunstancias que rodean la operación o la serie de operaciones de transferencia de datos y hayan ofrecido en su caso, sobre la base de dicha evaluación, garantías apropiadas con respecto a la protección de datos personales.

2. Una transferencia efectuada de conformidad con el apartado 1, letra g), no implicará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Cuando la finalidad del registro sea la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o cuando ellas sean las destinatarias.

3. Cuando el tratamiento se efectúe de conformidad con el apartado 1, letra h), el responsable o el encargado del tratamiento prestarán especial atención a la naturaleza de los datos, la finalidad y la duración de la operación o las operaciones de tratamiento propuestas, así como la situación en el país de origen, el tercer país y el país de destino final, y ofrecerán, en su caso, garantías apropiadas con respecto a la protección de datos personales.

4. Las letras b), c) y h) del apartado 1 no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

5. El interés público contemplado en el apartado 1, letra d), deberá ser reconocido por el Derecho de la Unión o del Estado miembro a que esté sujeto el responsable del tratamiento.

6. El responsable o el encargado del tratamiento documentarán, en la documentación contemplada en el artículo 28, la evaluación y las garantías apropiadas ofrecidas contempladas en el apartado 1, letra h), e informarán de la transferencia a la autoridad de control.

7. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los «motivos importantes de interés público» a tenor de lo dispuesto en el apartado 1, letra d), así como los criterios y requisitos aplicables a las garantías apropiadas contempladas en el apartado 1, letra h).

Artículo 45

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 las autoridades de control 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 41, apartado 3.

CAPÍTULO VI
AUTORIDADES DE CONTROL INDEPENDIENTES

SECCIÓN 1
INDEPENDENCIA

Artículo 46
Autoridad de control

1. Cada Estado miembro dispondrá que una o varias autoridades públicas se encarguen de supervisar la aplicación del presente Reglamento 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. 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, y establecerá un mecanismo para garantizar el cumplimiento por parte de las demás autoridades de las normas relativas al mecanismo de coherencia contemplado en el artículo 57.

3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el presente capítulo, a más tardar en la fecha especificada en el artículo 91, apartado 2, y, sin demora, cualquier modificación posterior que les afecte.

Artículo 47
Independencia

1. La autoridad de control actuará con total independencia en el ejercicio de las funciones que le hayan sido encomendadas y de los poderes que le hayan sido conferidos.

2. 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 los locales y las infraestructuras necesarios 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 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 48

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, en particular en el ámbito de la protección de datos personales.

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 49

Normas relativas al establecimiento de la autoridad de control

Cada Estado miembro dispondrá por ley, dentro de los límites del presente Reglamento:

a) el establecimiento y el estatuto de la autoridad de control;

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 del presente Reglamento, algunos de los cuales podrán ser más breves cuando ello sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramientos escalonados;

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 en caso de que dejen de cumplir las condiciones requeridas para el ejercicio de sus funciones o incurrieran en falta grave.

Artículo 50
Secreto profesional

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 51
Competencia

1. Cada autoridad de control ejercerá, en el territorio de su propio Estado miembro, los poderes que se le confieran de conformidad con el presente Reglamento.

2. Cuando el tratamiento de los datos personales tenga lugar en el marco de las actividades de un responsable o un encargado del tratamiento establecidos en la Unión, y el responsable o el encargado estén establecidos en varios Estados miembros, la autoridad de control del Estado miembro en que esté situado el establecimiento principal del responsable o del encargado será competente para controlar las actividades de tratamiento del responsable o del encargado en todos los

Estados miembros, sin perjuicio de lo dispuesto en el capítulo VII del presente Reglamento.

3. 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 52
Funciones

1. La autoridad de control:

a) supervisará y asegurará la aplicación del presente Reglamento;

b) conocerá las reclamaciones presentadas por cualquier interesado o por una asociación que le represente de conformidad con lo dispuesto en el artículo 73, investigará, en la medida en que proceda, el asunto e informará al interesado o a 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) compartirá información con otras autoridades de control, les prestará asistencia mutua y velará por la coherencia en la aplicación del presente Reglamento para garantizar su cumplimiento;

d) 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;

e) 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 y de las prácticas comerciales;

f) 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;

g) autorizará las operaciones de tratamiento contempladas en el artículo 34 y será consultado sobre las mismas;

h) emitirá un dictamen sobre los proyectos de código de conducta de conformidad con lo dispuesto en el artículo 38, apartado 2;

i) aprobará normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 43;

j) 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 confiere el presente Reglamento 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. El desempeño de las funciones de la autoridad de control será gratuito para el interesado.

6. Cuando las solicitudes sean manifiestamente excesivas, 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 manifiestamente excesivo de la solicitud recaerá en la autoridad de control.

Artículo 53
Poderes

1. Cada autoridad de control estará facultada para:

a) notificar al responsable o al encargado del tratamiento una presunta violación de las disposiciones que rigen el tratamiento de datos personales y, cuando proceda, ordenar al responsable o al encargado que subsanen dicha violación, de manera específica, con el fin de mejorar la protección del interesado;

b) ordenar al responsable o al encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos conferidos por el presente Reglamento presentadas por el interesado;

c) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante que faciliten cualquier información útil para el desempeño de sus funciones;

d) velar por el cumplimiento de las autorizaciones y consultas previas contempladas en el artículo 34;

e) formular una advertencia o amonestación al responsable o al encargado del tratamiento;

f) ordenar la rectificación, supresión o destrucción de todos los datos que se hayan tratado infringiendo las disposiciones del presente Reglamento, y la notificación de dichas medidas a los terceros a quienes se hayan comunicado los datos;

g) prohibir temporal o definitivamente el tratamiento;

h) suspender los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional;

i) emitir dictámenes sobre cualquier cuestión relacionada con la protección de datos personales;

j) informar al parlamento nacional, al gobierno o a otras instituciones políticas, así como al público, sobre cualquier cuestión relacionada con la protección de datos personales.

2. Cada autoridad de control dispondrá de poderes de investigación que le permitan obtener del responsable o del encargado del tratamiento:

a) el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

b) el acceso a todos sus locales, en particular cualquier equipamiento y medio de tratamiento de datos, cuando haya motivos razonables para suponer que en ellos se ejerce una actividad contraria al presente Reglamento.

Los poderes contemplados en la letra b) serán ejercidos de conformidad con el Derecho de la Unión y el Derecho de los Estados miembros.

3. Cada autoridad de control estará facultada para poner en conocimiento de las autoridades judiciales las violaciones de las disposiciones del presente Reglamento y para ejercitar acciones jurisdiccionales, en particular de conformidad con lo dispuesto en el artículo 74, apartado 4, y en el artículo 75, apartado 2.

4. Cada autoridad de control estará facultada para sancionar las infracciones administrativas, en particular las contempladas en el artículo 79, apartados 4, 5 y 6.

Artículo 54
Informe de actividad

Cada autoridad de control deberá elaborar un informe anual sobre sus actividades. El informe será presentado al parlamento nacional y se pondrá a disposición del público, de la Comisión y del Consejo Europeo de Protección de Datos.

CAPÍTULO VII
COOPERACIÓN Y COHERENCIA

SECCIÓN 1
COOPERACIÓN

Artículo 55
Asistencia mutua

1. Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua a fin de implementar y aplicar el presente Reglamento de manera 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 de autorización y consulta previas, las inspecciones y la comunicación rápida de información sobre la apertura de expedientes y su evolución, cuando sea probable que las operaciones de tratamiento afecten a interesados en varios Estados miembros.

2. Cada autoridad de control adoptará todas las medidas apropiadas requeridas para responder a la solicitud de otra autoridad de control sin demora y a más tardar en el plazo de un mes tras haber recibido la solicitud. Podrá tratarse, en particular, de la transmisión de información útil sobre el curso de una investigación o medidas represivas para que se proceda al cese o a la prohibición de las operaciones de tratamiento contrarias al presente Reglamento.

3. La solicitud de asistencia deberá contener toda la información necesaria, sobre todo la finalidad y los motivos de la solicitud. La información intercambiada se utilizará únicamente para los fines para la que se solicitó.

4. Una autoridad de control a la que se haya dirigido una solicitud de asistencia no podrá negarse a atenderla, salvo si:

   a) no fuera competente para dar curso a la solicitud; o

   b) el hecho de atender la solicitud fuera incompatible con las disposiciones del presente Reglamento.

5. La autoridad de control a la que se haya dirigido la solicitud 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.

6. Las autoridades de control facilitarán la información solicitada por otras autoridades de control por vía electrónica y en el plazo más breve posible, utilizando un formato normalizado.

7. No se cobrará tasa alguna por las medidas adoptadas a raíz de una solicitud de asistencia mutua.

8. Cuando una autoridad de control no actúe en el plazo de un mes a solicitud de otra autoridad de control, la autoridad de control solicitante será competentes para adoptar una medida provisional en el territorio de su Estado miembro de conformidad con lo dispuesto en el artículo 51, apartado 1, y someterá el asunto al Consejo Europeo de Protección de Datos de conformidad con el procedimiento contemplado en el artículo 57.

9. La autoridad de control especificará el plazo de validez de dicha medida provisional. Dicho plazo no excederá de tres meses. La autoridad de control comunicará sin demora dichas medidas, debidamente motivadas, al Consejo Europeo de Protección de Datos y a la Comisión.

10. La Comisión podrá especificar el formato y los procedimientos de asistencia mutua contemplados en el presente artículo, así como las modalidades del intercambio de información por vía electrónica entre las autoridades de control y entre las autoridades de control y el Consejo Europeo de Protección de Datos, en especial el formato normalizado contemplado en el apartado 6. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

Artículo 56
Operaciones conjuntas de las autoridades de control

1. Con el fin de intensificar la cooperación y la asistencia mutua, las autoridades de control llevarán a cabo tareas de investigación conjuntas, medidas represivas conjuntas y otras operaciones conjuntas en las que participen miembros designados o personal de las autoridades de control de otros Estados miembros.

2. En los casos en que sea probable que se vean afectados por las operaciones de tratamiento interesados en varios Estados miembros, tendrá derecho a participar en las tareas de investigación conjuntas o en las operaciones conjuntas, según proceda, una autoridad de control de cada uno de esos Estados miembros. La autoridad de control competente invitará a la autoridad de control de cada uno de esos Estados miembros a tomar parte en las tareas de investigación conjuntas o en las operaciones conjuntas de que se trate y responderá sin demora a la solicitud de una autoridad de control que desee participar en las operaciones.

3. En su calidad de autoridad de control de acogida, cada autoridad de control podrá, con arreglo a su Derecho interno y con la autorización de la autoridad de control de origen, conferir competencias de ejecución, en particular tareas de investigación, a los miembros o al personal de la autoridad de control de origen que participen en operaciones conjuntas o aceptar, en la medida en que lo permita la legislación de la autoridad de control de acogida, que los miembros o el personal de la autoridad de control de origen ejerzan sus competencias de ejecución de conformidad con la legislación de la autoridad de control de origen. Dichas competencias de ejecución solo podrán ejercerse bajo la orientación y, por regla general, en presencia de miembros o personal de la autoridad de control de acogida. Los miembros o el personal de la autoridad de control de origen estarán sujetos al Derecho interno de la autoridad de control de acogida. La autoridad de control de acogida asumirá la responsabilidad de sus actos.

4. Las autoridades de control establecerán los aspectos prácticos de las acciones de cooperación específicas.

5. Cuando una autoridad de control no cumpla en el plazo de un mes la obligación establecida en el apartado 2, las demás autoridades de control serán competentes para adoptar una medida provisional en el territorio de su Estado miembro, de conformidad con lo dispuesto en el artículo 51, apartado 1.

6. La autoridad de control especificará el plazo de validez de toda medida provisional contemplada en el apartado 5. Dicho plazo no excederá de tres meses. La autoridad de control comunicará sin demora dichas medidas, debidamente motivadas, al Consejo Europeo de Protección de Datos y a la Comisión y someterá el asunto al mecanismo contemplado en el artículo 57.

SECCIÓN 2
COHERENCIA

Artículo 57
Mecanismo de coherencia

Para los fines establecidos en el artículo 46, apartado 1, las autoridades de control cooperarán entre sí y con la Comisión, en el marco del mecanismo de coherencia, como se dispone en la presente sección.

Artículo 58
Dictamen del Consejo Europeo de Protección de Datos

1. Antes de adoptar una medida contemplada en el apartado 2, las autoridades de control comunicarán el proyecto de medida al Consejo Europeo de Protección de Datos y a la Comisión.

2. La obligación establecida en el apartado 1 se aplicará a cualquier medida destinada a producir efectos jurídicos que:

   a) ataña a actividades de tratamiento relacionadas con la oferta de bienes o servicios a interesados en varios Estados miembros o con el control de su comportamiento; o

   b) pueda afectar sustancialmente a la libre circulación de datos personales dentro de la Unión; o

   c) tenga por objeto la adopción de una lista de las operaciones de tratamiento que deben ser objeto de consulta previa de conformidad con lo dispuesto en el artículo 34, apartado 5; o

   d) tenga por objeto la determinación de las cláusulas tipo de protección de datos contempladas en el artículo 42, apartado 2, letra c); o

e) tenga por objeto la autorización de las cláusulas tipo contempladas en el artículo 42, apartado 2, letra d); o

f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor de lo dispuesto en el artículo 43.

3. Las autoridades de control o el Consejo Europeo de Protección de Datos podrán solicitar que cualquier asunto sea tratado en el marco del mecanismo de coherencia, en particular cuando una autoridad de control no presente un proyecto de medida contemplado en el apartado 2 o no cumpla las obligaciones relativas a la asistencia mutua de conformidad con lo dispuesto en el artículo 55 o a las operaciones conjuntas de conformidad con lo dispuesto en el artículo 56.

4. A fin de garantizar la aplicación correcta y coherente del presente Reglamento, la Comisión podrá solicitar que cualquier asunto sea tratado en el marco del mecanismo de coherencia.

5. Las autoridades de control y la Comisión comunicarán por vía electrónica y utilizando un formato normalizado toda información útil, en particular, cuando proceda, un resumen de los hechos, el proyecto de medida y los motivos por los que es necesaria su adopción.

6. El presidente del Consejo Europeo de Protección de Datos informará inmediatamente por vía electrónica a los miembros del Consejo Europeo de Protección de Datos y a la Comisión de cualquier información útil que le haya sido comunicada, utilizando un formato normalizado. El presidente del Consejo Europeo de Protección de Datos facilitará, de ser sea necesario, traducciones de la información útil.

7. El Consejo Europeo de Protección de Datos emitirá un dictamen sobre el asunto si así lo decide por mayoría simple de sus miembros o si cualquier autoridad de control o la Comisión lo solicitan en el plazo de una semana después de que se haya facilitado la información útil con arreglo a lo dispuesto en el apartado 5. El dictamen se adoptará en el plazo de un mes por mayoría simple de los miembros del Consejo Europeo de Protección de Datos. El presidente del Consejo Europeo de Protección de Datos informará del dictamen, sin demora injustificada, a la autoridad de control contemplada, según proceda, en los apartados 1 y 3, a la Comisión y a la autoridad de control competente en virtud del artículo 51, y lo hará público.

8. La autoridad de control contemplada en el apartado 1 y la autoridad de control competente en virtud del artículo 51 tendrán en cuenta el dictamen del Consejo Europeo de Protección de Datos y, en el plazo de dos semanas desde que el presidente del Consejo Europeo de Protección de Datos haya informado sobre el dictamen, comunicarán por vía electrónica a dicho presidente y a la Comisión si mantienen o modifican su proyecto de medida y, si lo hubiera, el proyecto de medida modificado, utilizando para ello un formato normalizado.

Artículo 59
Dictamen de la Comisión

1. En el plazo de diez semanas a partir de que se haya planteado un asunto en virtud del artículo 58 o, a más tardar, en el plazo de seis semanas en el caso contemplado en el

artículo 61, la Comisión podrá adoptar, para garantizar la aplicación correcta y coherente del presente Reglamento, un dictamen sobre los asuntos planteados con arreglo a lo dispuesto en los artículos 58 o 61.

2. Cuando la Comisión haya adoptado un dictamen de conformidad con lo dispuesto en el apartado 1, la autoridad de control afectada tendrá debidamente en cuenta el dictamen de la Comisión e informará a la Comisión y al Consejo Europeo de Protección de Datos su intención de mantener o modificar su proyecto de medida.

3. Durante el plazo contemplado en el apartado 1, la autoridad de control se abstendrá de adoptar el proyecto de medida.

4. Cuando la autoridad de control interesada no tenga intención de atenerse al dictamen de la Comisión, informará de ello a la Comisión y al Consejo Europeo de Protección de Datos en el plazo contemplado en el apartado 1 y motivará su decisión. En este caso, el proyecto de medida no podrá adoptarse durante un plazo adicional de un mes.

Artículo 60
Suspensión de un proyecto de medida

1. En el plazo de un mes a partir de la comunicación contemplada en el artículo 59, apartado 4, y cuando la Comisión tenga serias dudas en cuanto a si el proyecto de medida permitirá garantizar la correcta aplicación del presente Reglamento o si, por el contrario, resultará en una aplicación incoherente del mismo, la Comisión podrá adoptar una decisión motivada por la que exija a la autoridad de control que suspenda la adopción del proyecto de medida, teniendo en cuenta el dictamen emitido por el Consejo Europeo de Protección de Datos de conformidad con lo dispuesto en el artículo 59, apartado 7, o en el artículo 61, apartado 2, cuando ello parezca necesario para:

   a) aproximar las posiciones divergentes de la autoridad de control y del Consejo Europeo de Protección de Datos, si aún parece posible; o

   b) adoptar una medida de conformidad con lo dispuesto en el artículo 62, apartado 1, letra a).

2. La Comisión especificará la duración de la suspensión, que no podrá exceder de doce meses.

3. Durante el periodo contemplado en el apartado 2, la autoridad de control no podrá adoptar el proyecto de medida.

Artículo 61
Procedimiento de urgencia

1. En circunstancias excepcionales, cuando una autoridad de control considere que es urgente intervenir para proteger los intereses de interesados, en particular cuando exista el peligro de que el ejercicio efectivo de un derecho de un interesado pueda verse considerablemente obstaculizado por una alteración de la situación existente, o

para evitar inconvenientes importantes o por otros motivos, podrá adoptar inmediatamente, como excepción al procedimiento contemplado en el artículo 58, medidas provisionales con un periodo de validez determinado. La autoridad de control comunicará sin demora dichas medidas, debidamente motivadas, al Consejo Europeo de Protección de Datos y a la Comisión.

2. Cuando una autoridad de control haya adoptado una medida de conformidad con lo dispuesto en el apartado 1, y considere que deben adoptarse urgentemente medidas definitivas, podrá solicitar con carácter urgente un dictamen del Consejo Europeo de Protección de Datos, motivando su solicitud, y en particular la urgencia de las medidas definitivas.

3. Cualquier autoridad de control podrá solicitar, motivando su solicitud y, en particular, la urgencia de la intervención, un dictamen urgente cuando la autoridad de control competente no haya tomado una medida apropiada en una situación en la que sea urgente intervenir a fin de proteger los intereses de los interesados.

4. No obstante lo dispuesto en el artículo 58, apartado 7, los dictámenes urgentes contemplados en los apartados 2 y 3 del presente artículo se adoptarán en el plazo de dos semanas por mayoría simple de los miembros del Consejo Europeo de Protección de Datos.

Artículo 62
Actos de ejecución

1. La Comisión podrá adoptar actos de ejecución para:

   a) decidir sobre la aplicación correcta del presente Reglamento de conformidad con sus objetivos y requisitos en relación con los asuntos comunicados por las autoridades de control con arreglo a lo dispuesto en los artículos 58 o 61, en lo tocante a un asunto en relación con el cual se haya adoptado una decisión motivada de conformidad con lo dispuesto en el artículo 60, apartado 1, o a un asunto en relación con el cual una autoridad de control no haya presentado un proyecto de medida y haya anunciado que no tiene intención de atenerse al dictamen de la Comisión adoptado de conformidad con lo dispuesto en el artículo 59;

   b) decidir, en el plazo contemplado en el artículo 59, apartado 1, si declara que el proyecto de cláusulas tipo de protección de datos contemplado en el artículo 58, apartado 2, la letra d), tiene validez general;

   c) especificar el formato y los procedimientos de aplicación del mecanismo de coherencia contemplado en la presente sección;

   d) especificar las modalidades de intercambio de información por vía electrónica entre las autoridades de control, y entre dichas autoridades y el Consejo Europeo de Protección de Datos, en especial el formato normalizado contemplado en el artículo 58, apartados 5, 6 y 8.

   Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.

2. Por razones de imperiosa urgencia debidamente justificadas relativas a los intereses de los interesados en los casos contemplados en el apartado 1, letra a), la Comisión adoptará inmediatamente actos de ejecución inmediatamente aplicables de conformidad con el procedimiento contemplado en el artículo 87, apartado 3. Estos actos estarán vigentes durante un periodo no superior a doce meses.

3. La ausencia o la adopción de una medida en virtud de la presente sección se entenderán sin perjuicio de cualquier otra medida adoptada por la Comisión en virtud de los Tratados.

Artículo 63
Ejecución

1. A efectos del presente Reglamento, toda medida ejecutoria adoptada por la autoridad de control de un Estado miembro se ejecutará en todos los Estados miembros afectados.

2. Cuando una autoridad de control no presente un proyecto de medida al mecanismo de coherencia, contrariamente a lo dispuesto en el artículo 58, apartados 1 a 5, la medida de la autoridad de control carecerá de validez jurídica y no tendrá carácter ejecutorio.

SECCIÓN 3
CONSEJO EUROPEO DE PROTECCIÓN DE DATOS

Artículo 64
Consejo Europeo de Protección de Datos

1. Se crea el Consejo Europeo de Protección de Datos.

2. El Consejo Europeo de Protección de Datos estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos.

3. Cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, estas nombrarán al director de una de ellas como representante común.

4. La Comisión tendrá derecho a participar en las actividades y reuniones del Consejo Europeo de Protección de Datos y designará un representante. El presidente del Consejo Europeo de Protección de Datos informará sin demora a la Comisión de todas las actividades del Consejo Europeo de Protección de Datos.

Artículo 65
Independencia

1. El Consejo Europeo de Protección de Datos actuará con total independencia en el ejercicio de las tareas que se le encomienden con arreglo a lo dispuesto en los artículos 66 y 67.

2. Sin perjuicio de las solicitudes de la Comisión contempladas en el apartado 1, letra b), y en el apartado 2 del artículo 66, en el ejercicio de sus tareas el Consejo Europeo de Protección de Datos no solicitará ni admitirá instrucciones de nadie.

Artículo 66
Tareas del Consejo Europeo de Protección de Datos

1. El Consejo Europeo de Protección de Datos velará por la aplicación coherente del presente Reglamento. A tal efecto, el Consejo Europeo de Protección de Datos, a iniciativa propia o a instancia de la Comisión, en particular:

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

   b) examinará, a iniciativa propia o a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del presente Reglamento, y emitirá directrices, recomendaciones y mejores prácticas dirigidas a las autoridades de control, a fin de promover la aplicación coherente del presente Reglamento;

   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 dictámenes sobre los proyectos de decisión de las autoridades de control con arreglo al mecanismo de coherencia contemplado en el artículo 57;

   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 sobre la legislación y las prácticas en materia de protección de datos con las autoridades de control de la protección de datos a escala mundial.

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 87, 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.

Artículo 67
Informes

1. El Consejo Europeo de Protección de Datos informará periódicamente y en su debido momento a la Comisión sobre el resultado de sus actividades. Elaborará un informe anual sobre la situación en materia de protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Unión y en terceros países.

   El informe incluirá el examen de la aplicación práctica de las directrices, recomendaciones y mejores prácticas contempladas en el artículo 66, apartado 1, letra c).

2. El informe se hará público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión.

Artículo 68
Procedimiento

1. El Consejo Europeo de Protección de Datos tomará sus decisiones por mayoría simple de sus miembros.

2. El Consejo Europeo de Protección de Datos adoptará su reglamento interno y sus disposiciones de funcionamiento. En concreto, adoptará disposiciones relativas a la continuidad del ejercicio de las funciones cuando dimita un miembro o expire su mandato, la creación de subgrupos para temas o sectores específicos y los procedimientos que aplicará en lo que respecta al mecanismo de coherencia contemplado en el artículo 57.

Artículo 69
Presidente

1. El Consejo Europeo de Protección de Datos elegirá de entre sus miembros un presidente y dos vicepresidentes. Uno de los vicepresidentes será el Supervisor Europeo de Protección de Datos, salvo que haya sido elegido presidente.

2. La duración del mandato del presidente y de los vicepresidentes será de cinco años renovables.

Artículo 70
Tareas del presidente

1. El presidente desempeñará las siguientes funciones:

   a) convocar las reuniones del Consejo Europeo de Protección de Datos y preparar su agenda;

   b) garantizar el cumplimiento puntual de las tareas del Consejo Europeo de Protección de Datos, en particular, en relación con el mecanismo de coherencia contemplado en el artículo 57.

2. El Consejo Europeo de Protección de Datos determinará la distribución de tareas entre el presidente y los vicepresidentes en su reglamento interno.

Artículo 71
Secretaría

1. El Consejo Europeo de Protección de Datos contará con una secretaría. El Supervisor Europeo de Protección de Datos se hará cargo de dicha secretaría.

2. La secretaría prestará apoyo analítico, administrativo y logístico al Consejo Europeo de Protección de Datos, bajo la dirección del presidente.

3. La secretaría será responsable, en particular, de:

   a) los asuntos corrientes del Consejo Europeo de Protección de Datos;

   b) la comunicación entre los miembros del Consejo Europeo de Protección de Datos, su presidente y la Comisión, así como de la comunicación con otras instituciones y con el público;

   c) la utilización de medios electrónicos para la comunicación interna y externa;

   d) la traducción de la información pertinente;

   e) la preparación y el seguimiento de las reuniones del Consejo Europeo de Protección de Datos;

   f) la preparación, redacción y publicación de dictámenes y otros textos adoptados por el Consejo Europeo de Protección de Datos.

Artículo 72
Confidencialidad

1. Los debates del Consejo Europeo de Protección de Datos serán confidenciales.

2. Los documentos presentados a los miembros del Consejo Europeo de Protección de Datos, los expertos y los representantes de terceras partes serán confidenciales, salvo que se conceda el acceso a dichos documentos de conformidad con el Reglamento

(CE) nº 1049/2001, o que el Consejo Europeo de Protección de Datos decida hacerlos públicos.

3. Los miembros del Consejo Europeo de Protección de Datos, los expertos y los representantes de terceras partes estarán obligados a respetar las obligaciones de confidencialidad dispuestas en el presente artículo. El presidente se cerciorará de que los expertos y los representantes de terceras partes tengan conocimiento de las obligaciones de confidencialidad que han de respetar.

CAPÍTULO VIII
RECURSOS, RESPONSABILIDAD Y SANCIONES

Artículo 73
Derecho a presentar una reclamación ante una autoridad de control

1. Sin perjuicio de los recursos administrativos o judiciales, todo interesado tendrá derecho 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 lo dispuesto en el presente Reglamento.

2. 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, tendrá derecho 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 les asisten en virtud del presente Reglamento han sido vulnerados como consecuencia del tratamiento de los datos personales.

3. Independientemente de la reclamación de un interesado, los organismos, organizaciones o asociaciones contemplados en el apartado 2 tendrán derecho a presentar una reclamación ante una autoridad de control en cualquier Estado miembro, si consideran que se ha producido una violación de los datos personales.

Artículo 74
Derecho a un recurso judicial contra una autoridad de control

1. Toda persona física o jurídica tendrá derecho a un recurso judicial contra las decisiones de una autoridad de control que le conciernan.

2. Todo 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 52, apartado 1, letra b).

3. 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.

4. El interesado que se vea afectado por una decisión de una autoridad de control de un Estado miembro en el que no tiene su residencia habitual podrá solicitar a la autoridad de control del Estado miembro en el que tiene su residencia habitual que ejercite en su nombre una acción contra la autoridad de control competente en el otro Estado miembro.

5. Los Estados miembros deberán ejecutar las resoluciones definitivas de los órganos jurisdiccionales mencionados en el presente artículo.

Artículo 75

Derecho a un recurso judicial contra un responsable o encargado

1. Sin perjuicio de los recursos administrativos disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control al que se refiere el artículo 73, las personas físicas tendrán derecho a un recurso judicial cuando consideren que los derechos que les asisten en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales no conforme con el presente Reglamento.

2. Las acciones contra un responsable o encargado deberán ejercitarse ante los órganos jurisdiccionales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los órganos jurisdiccionales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable sea una autoridad pública que actúa en ejercicio del poder público.

3. Cuando estuviere pendiente ante el mecanismo de coherencia contemplado en el artículo 58 un procedimiento referido a la misma medida, decisión o práctica, un órgano jurisdiccional podrá suspender el procedimiento incoado, salvo cuando la urgencia del asunto de que se trate para la protección de los derechos del interesado no permita esperar al resultado del procedimiento del mecanismo de coherencia.

4. Los Estados miembros deberán ejecutar las resoluciones definitivas de los órganos jurisdiccionales mencionados en el presente artículo.

Artículo 76

Normas comunes para los procedimientos judiciales

1. Todo organismo, organización o asociación a que se refiere el artículo 73, apartado 2, tendrá derecho a ejercer los derechos contemplados en los artículos 74 y 75 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 del presente Reglamento o de garantizar la coherencia de la protección de los datos personales en el territorio de la Unión.

3. Cuando un órgano jurisdiccional competente de un Estado miembro tenga motivos razonables para creer que se están llevando a cabo procedimientos paralelos en otro Estado miembro, se pondrá en contacto con el órgano jurisdiccional competente de dicho Estado miembro a fin de confirmar la existencia de tales procedimientos paralelos.

4. Cuando tales procedimientos paralelos en otro Estado miembro se refieran a la misma medida, decisión o práctica, el órgano jurisdiccional podrá suspender el procedimiento.

5. 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 77
Derecho a indemnización y responsabilidad

1. Toda persona que haya sufrido un perjuicio como consecuencia de una operación de tratamiento ilegal o de un acto incompatible con el presente Reglamento tendrá derecho a recibir del responsable o encargado del tratamiento una indemnización por el perjuicio sufrido.

2. En caso de que más de un responsable o encargado participe en el tratamiento, 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 78
Sanciones

1. Los Estados miembros establecerán normas sobre las sanciones aplicables a las infracciones de las disposiciones del presente Reglamento y adoptarán todas las medidas necesarias para garantizar su cumplimiento, incluso en el caso de que el responsable del tratamiento no cumpla la obligación de designar a un representante. Las sanciones establecidas deberán ser efectivas, proporcionadas y disuasorias.

2. Cuando el responsable del tratamiento haya designado un representante, cualquier sanción se impondrá a este último, sin perjuicio de las sanciones que pudieran promoverse contra el controlador.

3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1, a más tardar en la fecha especificada en el artículo 91, apartado 2, y, sin demora, cualquier modificación posterior de las mismas.

Artículo 79
Sanciones administrativas

1. Cada autoridad de control estará facultada para imponer sanciones administrativas de acuerdo con el presente artículo.

2. La sanción administrativa deberá ser efectiva, proporcionada y disuasoria en todos los casos. El importe de la multa administrativa se fijará teniendo en cuenta la naturaleza, gravedad y duración de la infracción, la intencionalidad o negligencia en la infracción, el grado de responsabilidad de la persona física o jurídica y anteriores infracciones de dicha persona, las medidas de carácter técnico y organizativo y los procedimientos aplicados de conformidad con el artículo 23, así como el grado de cooperación con la autoridad de control con el fin de reparar la infracción.

3. En el caso de un primer incumplimiento no deliberado del presente Reglamento, podrá enviarse una advertencia escrita y no se impondrá sanción alguna, si:

   a) una persona física realiza el tratamiento de datos personales sin interés comercial o,

   b) una empresa o una organización que emplee menos de 250 personas trata datos personales únicamente como actividad auxiliar de su actividad principal.

4. La autoridad de control impondrá una multa de hasta 250 000 EUR o, si se trata de una empresa, de hasta el 0,5 % de su volumen de negocios anual a nivel mundial, a toda persona que, de forma deliberada o por negligencia:

   a) no proporcione los mecanismos de solicitud de los interesados o no responda a tiempo o en el formato requerido a los interesados en virtud del artículo 12, apartados 1 y 2;

   b) imponga el pago de una tasa por la información o por las respuestas a las solicitudes de los interesados en incumplimiento de lo dispuesto en el artículo 12, apartado 4.

5. La autoridad de control impondrá una multa de hasta 500 000 EUR o, si se trata de una empresa, de hasta el 1 % de su volumen de negocios anual a nivel mundial, a todo aquel que, de forma deliberada o por negligencia:

   a) no facilite la información, o facilite información incompleta, o no facilite la información de una manera suficientemente transparente al interesado, de conformidad con el artículo 11, el artículo 12, apartado 3, y el artículo 14;

   b) no facilite el acceso a los datos por parte del interesado o no rectifique datos personales con arreglo a los artículos 15 y 16, o no comunique la información pertinente a un destinatario de conformidad con el artículo 13;

   c) no respete el derecho al olvido o a la supresión, no establezca mecanismos para garantizar el cumplimiento de los plazos o no tome todas las medidas necesarias para informar a los terceros de que un interesado les solicita que supriman cualquier vínculo a sus datos personales, o cualquier copia o réplica de los mismos, de conformidad con el artículo 17;

d) no facilite una copia de los datos personales en formato electrónico u obstaculice la transmisión de los datos personales por parte del interesado a otro sistema de tratamiento automatizado en violación del artículo 18;

e) no determine o determine insuficientemente las responsabilidades respectivas de los corresponsables con arreglo a lo dispuesto en el artículo 24;

f) no conserve documentación o no conserve la documentación suficiente con arreglo a lo dispuesto en el artículo 28, el artículo 31, apartado 4, y el artículo 44, apartado 3;

g) no cumpla, en los casos que no afecten a categorías especiales de datos, de acuerdo con los artículos 80, 82 y 83, las normas relativas a la libertad de expresión, las normas sobre el tratamiento de los datos en el ámbito laboral o las condiciones para el tratamiento de datos con fines de investigación histórica, estadística y científica.

6. La autoridad de control impondrá una multa de hasta 1 000 000 EUR o, si se trata de una empresa, de hasta el 2 % de su volumen de negocios anual a nivel mundial, a todo aquel que, de forma deliberada o por negligencia:

a) trate datos personales sin base jurídica o sin base jurídica suficiente para el tratamiento, o no cumpla las condiciones para el consentimiento con arreglo a los artículos 6, 7 y 8;

b) trate categorías especiales de datos personales en violación de los artículos 9 y 81;

c) no se allane a una oposición o a la obligación dispuesta en el artículo 19;

d) no cumpla las condiciones relativas a las medidas basadas en la elaboración de perfiles contempladas en el artículo 20;

e) no adopte políticas internas o no implemente medidas adecuadas para asegurar y demostrar la conformidad del tratamiento con los artículos 22, 23, y 30;

f) no designe a un representante en virtud del artículo 25;

g) trate o instruya el tratamiento de datos personales incumpliendo las obligaciones relativas al tratamiento por cuenta de un responsable del tratamiento contempladas en los artículos 26 y 27;

h) no alerte o no notifique una violación de datos personales o no notifique a tiempo o completamente la violación de datos personales a la autoridad de control o al interesado de acuerdo con los artículos 31 y 32;

i) no lleve a cabo una evaluación del impacto en la protección de datos o trate datos personales sin autorización o sin consulta previas de la autoridad de control con arreglo a los artículos 33 y 34;

j) no designe un agente de protección de datos o no garantice las condiciones para cumplir las tareas con arreglo a los artículos 35, 36 y 37;

k) haga un uso indebido de los sellos y marcas contemplados en el artículo 39;

l) lleve a cabo o instruya una transferencia de datos a un tercer país o a una organización internacional que no esté autorizada por una decisión de adecuación o por las garantías adecuadas o por alguna de las excepciones con arreglo a los artículos 40 a 44;

m) no cumpla un requerimiento o la prohibición temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 53, apartado1;

n) no cumpla las obligaciones de cooperación con la autoridad de control o no responda o no le facilite la información pertinente o el acceso a sus locales con arreglo al artículo 28, apartado 3, al artículo 29, al artículo 34, apartado 6, y al artículo 53, apartado 2;

o) no cumpla las normas de salvaguarda del secreto profesional con arreglo al artículo 84.

7. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a efectos de la actualización de los importes de las multas administrativas a que se hace referencia en los apartados 4, 5 y 6 del presente artículo, teniendo en cuenta los criterios indicados en el apartado 2.

CAPÍTULO IX
DISPOSICIONES RELATIVAS A SITUACIONES DE TRATAMIENTO DE DATOS ESPECÍFICAS

Artículo 80
Tratamiento de datos personales y libertad de expresión

1. Los Estados miembros dispondrán exenciones o excepciones a las disposiciones relativas a los principios generales del Capítulo II, los derechos del interesado del Capítulo III, el responsable y el encargado del Capítulo IV, la transferencia de datos personales a terceros países y a organizaciones internacionales del Capítulo V, las autoridades de control independientes del Capítulo VI y la cooperación y la coherencia del Capítulo VII en lo referente al tratamiento de los datos personales efectuado exclusivamente con fines periodísticos o de expresión literaria o artística, para conciliar el derecho a la protección de los datos de carácter personal con las normas que rigen la libertad de expresión.

2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1, a más tardar en la fecha especificada en el artículo 91, apartado 2, y, sin demora, cualquier modificación posterior modificación posterior de las mismas.

Artículo 81

Tratamiento de datos personales relativos a la salud

1. Dentro de los límites establecidos en el presente Reglamento y de conformidad con el artículo 9, apartado 2, letra h), el tratamiento de datos personales relativos a la salud deberá realizarse sobre la base del Derecho de la Unión o de los Estados miembros, que deberá establecer las disposiciones específicas adecuadas para salvaguardar los legítimos intereses del interesado, y deberá ser necesario:

   a) a los fines de la medicina preventiva o la medicina del trabajo, el diagnóstico médico, la prestación de asistencia sanitaria o el tratamiento o la gestión de los servicios de asistencia sanitaria, siempre que tales datos sean tratados por un profesional sanitario sujeto a la obligación del secreto profesional o por otra persona también sujeta a una obligación de confidencialidad equivalente en virtud de la legislación del Estado miembro o de las normas establecidas por los organismos nacionales competentes; o

   b) por razones de interés público en el ámbito de la salud pública, como la protección contra riesgos sanitarios transfronterizos graves, o para garantizar altos niveles de calidad y seguridad de los medicamentos o del material sanitario; o

   c) por otras razones de interés público en ámbitos como la protección social, especialmente a fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad.

2. El tratamiento de datos personales relativos a la salud que sea necesario para los fines de la investigación histórica, estadística o científica, como el establecimiento de registros de pacientes con el fin de mejorar el diagnóstico, distinguir entre tipos de enfermedades similares y preparar estudios para terapias, estará supeditado al cumplimiento de las condiciones y garantías contempladas en el artículo 83.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 87, a fin de especificar otras razones de interés público en el ámbito de la salud pública a que se refiere el apartado 1, letra b), así como los criterios y requisitos de las garantías del tratamiento de datos personales a los fines a que se hace referencia en el apartado 1.

Artículo 82

Tratamiento en el ámbito laboral

1. Dentro de los límites del presente Reglamento, los Estados miembros podrán adoptar por ley normas específicas que rijan el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular para la contratación de personal, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, la gestión, planificación y organización del trabajo, la salud y la seguridad en el trabajo, así como a los fines del ejercicio y disfrute, individuales o colectivos, de los derechos y prestaciones relacionados con el empleo y a efectos del cese de la relación laboral.

2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1, a más tardar en la fecha especificada en el artículo 91, apartado 2, y, sin demora, cualquier modificación posterior de las mismas.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 86, a fin de especificar los criterios y requisitos de las garantías del tratamiento de datos personales para los fines mencionados en el apartado 1.

Artículo 83

Tratamiento para fines de investigación histórica, estadística o científica

1. Dentro de los límites del presente Reglamento, podrán tratarse los datos personales para fines de investigación histórica, estadística o científica sólo si:

   a) dichos fines no pueden lograrse de otra forma mediante un tratamiento de datos que no permita o que ya no permita la identificación del interesado;

   b) los datos que permitan la atribución de información a un interesado identificado o identificable se conservan por separado del resto de la información, en la medida en que dichos fines puedan lograrse de este modo.

2. Los organismos que llevan a cabo investigaciones históricas, estadísticas o científicas podrán publicar o hacer públicos por otra vía datos personales sólo si:

   a) el interesado ha dado su consentimiento en las condiciones establecidas en el artículo 7;

   b) la publicación de los datos personales es necesaria para presentar los resultados de una investigación o para facilitar una investigación, siempre que los intereses o los derechos o libertades fundamentales del interesado no prevalezcan sobre tales objetivos; o

   c) el interesado ha hecho públicos los datos.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 86, a fin de especificar los criterios y requisitos del tratamiento de los datos personales a los efectos mencionados en los apartados 1 y 2, así como las limitaciones necesarias a los derechos de información y de acceso por parte del interesado, y de detallar las condiciones y garantías de los derechos del interesado en tales circunstancias.

Artículo 84

Obligaciones de secreto

1. Dentro de los límites del presente Reglamento, los Estados miembros podrán adoptar normas específicas para establecer los poderes de investigación de las autoridades de control contempladas en el artículo 53, apartado 2, en relación con los responsables o encargados sujetos, con arreglo al Derecho nacional o las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional u otras

obligaciones equivalentes de confidencialidad, cuando ello sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de confidencialidad. Estas normas solo se aplicarán a los datos personales que el responsable o el encargado hayan recibido u obtenido en una actividad cubierta por la citada obligación de confidencialidad.

2. Cada Estado miembro notificará a la Comisión las normas adoptadas de conformidad con el apartado 1, a más tardar en la fecha especificada en el artículo 91, apartado 2, y, sin demora, cualquier modificación posterior de las mismas.

Artículo 85

Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas

1. Cuando en un Estado miembro, iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del presente Reglamento, un conjunto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, tales normas podrán seguir aplicándose, siempre que sean conformes con las disposiciones del presente Reglamento.

2. Las iglesias y asociaciones religiosas que apliquen un conjunto de normas, de conformidad con el apartado 1, dispondrán la creación de una autoridad de control independiente, de conformidad con lo dispuesto en el Capítulo VI del presente Reglamento.

CAPÍTULO X
ACTOS DELEGADOS Y ACTOS DE EJECUCIÓN

Artículo 86

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 refieren el artículo 6, apartado 7, el artículo 8, apartado 3, el artículo 9, apartado 3, el 12, apartado 5, el artículo 14, apartado 7, el artículo 15, apartado 3, el artículo 17, apartado 9, el artículo 20, apartado 6, el artículo 22, apartado 4, el artículo 23, apartado 3, el artículo 26, apartado 5, el artículo 28, apartado 4, el artículo 30, apartado 3, el artículo 31, apartado 5, el artículo 32, apartado 5, el artículo 33, apartado 6, el artículo 34, apartado 8, el artículo 35, apartado 11, el artículo 37, apartado 2, el artículo 39, apartado 2, el artículo 43, apartado 3, el artículo 44, apartado 7, el artículo 79, apartado 6, el artículo 81, apartado 3, el artículo 82, apartado 3, y el artículo 83, apartado 3, se atribuirá a la Comisión por un periodo de tiempo indeterminado a partir de la fecha de entrada en vigor del presente Reglamento.

3. La delegación de poderes a que se refieren el artículo 6, apartado 5, el artículo 8, apartado 3, el artículo 9, apartado 3, el artículo 12, apartado 5, el artículo 14, apartado 7, el artículo 15, apartado 3, el artículo 17, apartado 9, el artículo 20, apartado 6, el artículo 22, apartado 4, el artículo 23, apartado 3, el artículo 26,

apartado 5, el artículo 28, apartado 5, el artículo 30, apartado 3, el artículo 31, apartado 5, el artículo 32, apartado 5, el artículo 33, apartado 6, el artículo 34, apartado 8, el artículo 35, apartado 11, el artículo 37, apartado 2, el artículo 39, apartado 2, el artículo 43, apartado 3, el artículo 44, apartado 7, el artículo 79, apartado 6, el artículo 81, apartado 3, el artículo 82, apartado 3, y en el artículo 83, apartado 3, podrá ser revocada en todo 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. Tan pronto como la Comisión adopte un acto delegado, lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Todo acto delegado adoptado en virtud del artículo 6, apartado 5, el artículo 8, apartado 3, el artículo 9, apartado 3, el 12, apartado 5, el artículo 14, apartado 7, el artículo 15, apartado 3, el artículo 17, apartado 9, el artículo 20, apartado 6, el artículo 22, apartado 4, el artículo 23, apartado 3, el artículo 26, apartado 5, el artículo 28, apartado 5, el artículo 30, apartado 3, el artículo 31, apartado 5, el artículo 32, apartado 5, el artículo 33, apartado 6, el artículo 34, apartado 8, el artículo 35, apartado 11, el artículo 37, apartado 2, el artículo 39, apartado 2, el artículo 43, apartado 3, el artículo 44, apartado 7, el artículo 79, apartado 6, el artículo 81, apartado 3, el artículo 82, apartado 3 y el artículo 83, apartado 3, 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 87
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 XI
DISPOSICIONES FINALES

Artículo 88
Derogación de la Directiva 95/46/CE

1. Queda derogada la Directiva 95/46/CE.

2. Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Consejo Europeo de Protección de Datos, establecido por el presente Reglamento.

Artículo 89
Relación con la Directiva 2002/58/CE y modificación de la misma

1. El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento de datos personales en relación con la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetos a obligaciones específicas con el mismo objetivo establecidos en la Directiva 2002/58/CE.

2 Queda suprimido el apartado 2 del artículo 1 de la Directiva 2002/58/CE.

Artículo 90
Evaluación

La Comisión presentará informes periódicos sobre la evaluación y revisión del presente Reglamento al Parlamento Europeo y al Consejo. El primer informe se presentará a más tardar cuatro años después de la entrada en vigor del presente Reglamento. Los siguientes informes se presentarán cada cuatro años. La Comisión presentará, si procede, las propuestas oportunas para modificar el presente Reglamento, y para adaptar otros instrumentos jurídicos, en particular teniendo en cuenta la evolución de las tecnologías de la información y a la luz de los progresos de la sociedad de la información. Dicho informe se hará público.

Artículo 91
Entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

2. Será aplicable a partir de [*dos años a partir de la fecha a que se refiere el apartado 1*].

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 25.1.2012

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

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

1.2. Ámbito(s) político(s) afectado(s) en la estructura GPA/PPA

1.3. Naturaleza de la propuesta/iniciativa

1.4. Objetivo(s)

1.5. Justificación de la propuesta/iniciativa

1.6. Duración e incidencia financiera

1.7. Modo(s) de gestión previsto(s)

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

2.2. Sistema de gestión y de control

2.3. Medidas de prevención de fraudes e irregularidades

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

3.2. Incidencia estimada en los gastos

3.2.1. Síntesis de la incidencia estimada en los gastos

3.2.2. Incidencia estimada en los créditos de operaciones

3.2.3. Incidencia estimada en los créditos administrativos

3.2.4. Compatibilidad con el marco financiero plurianual actual

3.2.5. Contribución de terceros a la financiación

3.3. Estimated impact on revenue

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

La presente ficha financiera indica con más detalle los requisitos en términos de gastos administrativos de la puesta en práctica de la reforma de la protección de datos, como se explica en la correspondiente evaluación de impacto. La reforma incluye dos propuestas legislativas, un Reglamento general de protección de datos y una Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales. La presente ficha financiera se refiere al impacto presupuestario de ambos instrumentos.

En función de la distribución de tareas, son necesarios recursos tanto para la Comisión como para el Supervisor Europeo de Protección de Datos (SEPD).

Por lo que se refiere a la Comisión, los recursos necesarios ya están incluidos en la propuesta de perspectivas financieras 2014-2020. La protección de datos es uno de los objetivos del programa «Derechos y Ciudadanía», que apoyará asimismo medidas para poner en práctica el marco jurídico. Los créditos administrativos, incluidas las necesidades de personal, se incluyen en el presupuesto administrativo de la DG JUST.

En cuanto al SEPD, se deberán tener en cuenta los recursos necesarios en sus respectivos presupuestos anuales. Los recursos se detallan en el anexo de la presente ficha financiera. Con el fin de dotar de los recursos necesarios a las nuevas tareas del Consejo Europeo de Protección de Datos, cuya secretaría asumirá el SEPD, será precisa una reprogramación de la rúbrica 5 de las perspectivas financieras 2014-2020.

1.1. *Denominación de la propuesta/iniciativa*

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).

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 delitos o la ejecución de sanciones penales, y a la libre circulación de estos datos.

1.2. *Ámbito(s) político(s) afectado(s) en la estructura GPA/PPA*[49]

Justicia - Protección de datos personales

[49] GPA: gestión por Actividades – PPA: presupuestación por actividades.

El impacto presupuestario se refiere a la Comisión y al SEPD. El impacto en el presupuesto de la Comisión es el que se detalla en los cuadros de la presente ficha financiera. Los gastos operativos forman parte del programa «Derechos y Ciudadanía» y ya se han tenido en cuenta en la ficha financiera del mismo, ya que los gastos administrativos forman parte de la dotación de la DG Justicia. Los elementos que afectan al SEPD figuran en el anexo.

1.3. *Naturaleza de la propuesta/iniciativa*

☐ La propuesta/iniciativa se refiere a una **acción nueva**

☐ La propuesta/iniciativa se refiere a una **acción nueva a raíz de un proyecto piloto / una acción preparatoria**[50]

☑ La propuesta/iniciativa se refiere a la **prolongación de una acción existente**

☐ La propuesta/iniciativa se refiere a **una acción reorientada hacia una nueva acción**

1.4. *Objetivos*

1.4.1. ***Objetivo(s) estratégico(s) plurianual(es) de la Comisión contemplado(s) en la propuesta/iniciativa***

La reforma tiene por objeto finalizar la realización de los objetivos iniciales, teniendo en cuenta nuevos progresos y retos, es decir:

- aumentar la eficacia del derecho fundamental a la protección de los datos y otorgar a los interesados el control de sus propios datos, en particular en el contexto de la evolución tecnológica y la creciente globalización;

- mejorar la dimensión de mercado interior de la protección de datos reduciendo la fragmentación, reforzando la coherencia y simplificando el entorno reglamentario, lo que permite eliminar gastos innecesarios y reducir la carga administrativa.

Además, la entrada en vigor del Tratado de Lisboa y, en particular, la introducción de una nueva base jurídica (artículo 16 del TFUE), ofrece la oportunidad de conseguir un nuevo objetivo, es decir,

- establecer un marco exhaustivo de protección de datos que cubra todas las áreas.

[50] Tal como se contempla en el artículo 49, apartado 6, letra a) o b), del Reglamento financiero.

1.4.2. ***Objetivo(s) específico(s) y actividad(es) GPA/PPA afectada(s)***

Objetivo específico nº 1

Para garantizar la aplicación coherente de las normas de protección de datos

Objetivo específico nº 2

Para racionalizar el actual sistema de gobernanza para garantizar una ejecución más coherente

Actividad(es) GPA/PPA afectada(s)

[…]

1.4.3. ***Resultado(s) e incidencia esperados***

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / la población destinataria.

Por lo que se refiere a los responsables del tratamiento de datos, las entidades públicas y privadas se beneficiarán de una mayor seguridad jurídica gracias a la armonización y clarificación de las normas y procedimientos de protección de datos de la UE, lo que permitirá garantizar las mismas condiciones y la aplicación coherente de las normas de protección de datos, así como una reducción considerable de la carga administrativa.

Las personas tendrán un mejor control de sus datos personales, lo que aumentará su confianza en el entorno digital, y seguirán estando protegidas incluso cuando sus datos personales se traten en el extranjero. También se beneficiarán de un refuerzo de la responsabilidad de los encargados del tratamiento de datos personales.

Un sistema de protección de datos exhaustivo cubrirá también los ámbitos de la policía y de la justicia, incluido el antiguo tercer pilar ampliado.

1.4.4. ***Indicadores de resultados e incidencia***

Especifíquense los indicadores que permiten realizar el seguimiento de la ejecución de la propuesta/iniciativa.

(véase la evaluación de impacto, punto 8)

Los indicadores se evaluarán periódicamente y se incluirán los siguientes elementos:

- Tiempo y costes dedicados por los responsables del tratamiento de datos al cumplimiento de la legislación de «otros Estados miembros»
- Recursos asignados a las autoridades responsables de la protección de datos
- Delegados de protección de datos designados de organizaciones públicas y privadas
- Uso hecho de la evaluación del impacto sobre la protección de datos
- Número de reclamaciones formuladas por los interesados e indemnizaciones recibidas por los interesados
- Número de casos que dan lugar a enjuiciamiento de los responsables de datos
- Multas impuestas a los responsables del tratamiento de datos competentes por infracciones de la protección de datos.

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo

Las actuales divergencias en la interpretación, aplicación y cumplimiento de la Directiva por parte de los Estados miembros ***obstaculizan el funcionamiento del mercado interior y la cooperación entre las autoridades públicas en relación con las políticas de la UE***. Esta situación contradice el objetivo fundamental de la Directiva de facilitar la libre circulación de

datos personales en el mercado interior. El rápido desarrollo de las nuevas tecnologías y de la globalización no hace sino exacerbar el problema.

Las personas físicas disfrutan de derecho de protección de datos diferentes debido a la fragmentación y a la incongruente aplicación y ejecución de la legislación en los distintos Estados miembros. Además, ***las personas físicas a menudo no saben lo que pasa con sus datos personales y no tienen ningún tipo de control sobre ellos*** y por lo tanto no llegan a ejercer sus derechos de forma efectiva.

1.5.2. Valor añadido de la intervención de la Unión Europea

Por sí solos, los Estados miembros no pueden mitigar los problemas que se plantean en la situación actual. Este es el caso, en particular, de los que se derivan de la fragmentación de las legislaciones nacionales de aplicación del marco regulador de la UE por lo que se refiere a la protección de datos. Por lo tanto, existen sólidas razones que justifican un marco jurídico para la protección de datos a nivel de la UE. 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 para todas las personas en la UE.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

La presente propuesta se basa en la experiencia adquirida con la Directiva 95/46/CE y responde a los problemas derivados de la transposición y aplicación fragmentadas de dicha Directiva, que impidieron lograr el doble objetivo de alcanzar un elevado nivel de protección de datos y establecer un mercado único para la protección de datos.

1.5.4. Compatibilidad y posible sinergia con otros instrumentos financieros.

El presente paquete legislativo de reforma de la protección de datos tiene por objetivo establecer un marco sólido, coherente y moderno en materia de protección de datos a escala de la UE, tecnológicamente neutro y válido para las próximas décadas. Beneficiará a las personas físicas – mediante el refuerzo de sus derechos en materia de protección de datos, en particular en un entorno digital – y simplificará el entorno legal para las empresas y el sector público, lo que permitirá estimular el desarrollo de la economía digital en el mercado interior de la UE y más allá de sus fronteras, en consonancia con los objetivos de la estrategia Europa 2020.

El núcleo del paquete legislativo de reforma de la protección de datos consta de:

– un Reglamento que sustituye a la Directiva 95/46/CE;

– una 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 delitos o la ejecución de sanciones penales, y a la libre circulación de estos datos.

Estas propuestas legislativas vienen acompañadas por un informe sobre la aplicación por los Estados miembros del que es hoy el principal instrumento de protección de datos de la UE en

los ámbitos de la cooperación policial y judicial en materia penal, la Decisión Marco 2008/977/JAI.

1.6. *Duración e incidencia financiera*

☐ Propuesta/iniciativa de **duración limitada**

– ☐ Propuesta/iniciativa en vigor desde el [DD/MM]AAAA hasta el [DD/MM]AAAA

– ☐ Incidencia financiera desde AAAA hasta AAAA

☑ Propuesta/iniciativa de **duración ilimitada**

– Ejecución con una fase de puesta en marcha desde 2014 hasta 2016,

– seguida de un pleno funcionamiento.

1.7. *Modo(s) de gestión previsto(s)*[51]

☑ **Gestión centralizada directa** a cargo de la Comisión

☐ **Gestión centralizada indirecta** mediante delegación de las tareas de ejecución en:

– ☐ agencias ejecutivas

– ☐ organismos creados por las Comunidades[52]

– ☐ organismos nacionales del sector público / organismos con misión de servicio público

– ☐ personas a quienes se haya encomendado la ejecución de acciones específicas de conformidad con el título V del Tratado de la Unión Europea y que estén identificadas en el acto de base correspondiente a efectos de lo dispuesto en el artículo 49 del Reglamento financiero

☐ **Gestión compartida** con los Estados miembros

☐ **Gestión descentralizada** con terceros países

☐ **Gestión conjunta** con organizaciones internacionales ***(especifíquense)***

Si se indica más de un modo de gestión, facilítense los detalles en el recuadro de observaciones.

Observaciones

//

[51] Las explicaciones sobre los modos de gestión y las referencias al Reglamento financiero pueden consultarse en el sitio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[52] Tal como se contemplan en el artículo 185 del Reglamento financiero.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones.

La primera evaluación tendrá lugar 4 años después de la entrada en vigor de los instrumentos jurídicos. En los instrumentos jurídicos se incluye una cláusula de revisión explícita, por la cual la Comisión evaluará su aplicación. A continuación, la Comisión informará al Parlamento Europeo y al Consejo sobre su evaluación. Se llevarán a cabo evaluaciones periódicas cada cuatro años. Se aplicará la metodología de evaluación de la Comisión. Estas evaluaciones se llevarán a cabo con la ayuda de estudios específicos sobre la aplicación de los instrumentos jurídicos, cuestionarios dirigidos a las autoridades nacionales de protección de datos, reuniones de expertos, talleres, encuestas del Eurobarómetro, etcétera.

2.2. Sistema de gestión y de control

2.2.1. Riesgo(s) definido(s)

Se ha llevado a cabo una evaluación del impacto de la reforma del marco de protección de datos en la UE que acompaña las propuestas de Reglamentos y de Directiva

El nuevo instrumento jurídico introducirá un mecanismo de coherencia que garantice la aplicación sistemática y coherente del marco por parte de autoridades independientes de control de los Estados miembros. El mecanismo funcionará a través del Consejo Europeo de Protección de Datos, integrado por los directores de las autoridades nacionales de control y el Supervisor Europeo de Protección de Datos (SEPD), que sustituirá al actual Grupo de Trabajo del artículo 29. El SEPD asumirá la secretaría de este organismo.

En caso de posibles decisiones divergentes por parte de las autoridades de los Estados miembros, se pedirá al Consejo Europeo de Protección de Datos que emita un dictamen sobre el asunto. Si este procedimiento fracasara, o si una autoridad de control se negara a cumplir con el dictamen, la Comisión podría, a fin de garantizar una aplicación correcta y coherente del presente Reglamento, emitir un dictamen o, en caso necesario, adoptar una decisión, si albergara serias dudas de que el proyecto de medida pueda garantizar la correcta aplicación del presente Reglamento, o pueda dar lugar a una aplicación incoherente.

El mecanismo de coherencia requiere la asignación de recursos adicionales al SEDP (12 EJC y los créditos operativos y administrativos adecuados, por ejemplo, para sistemas y tratamientos informáticos), de modo que pueda asumir la Secretaría, y a la Comisión (5 EJC y los créditos operativos y administrativos correspondientes), para el tratamiento de los casos de coherencia.

*2.2.2. **Medio(s) de control previsto(s)***

Los métodos de control existentes aplicados por el SEPD y por la Comisión abarcarán los créditos adicionales.

2.3. Medidas de prevención de fraudes e irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas.

Las medidas de prevención de fraudes existentes aplicadas por el SEPD y por la Comisión cubrirán los créditos adicionales.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. *Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)*

- Líneas presupuestarias de gasto existentes

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de **gasto**	Contribución			
	Número [Descripción … … …… … ….. … …. ….]	CD/CND (53)	**de países de la AELC**[54]	de países candidatos [55]	de terceros países	a efectos de lo dispuesto en el artículo 18.1.a bis) del Reglamento financiero

53 Disoc. = créditos disociados / no disoc. = créditos no disociados.

54 AELC: Asociación Europea de Libre Comercio.

55 Países candidatos y, en su caso, países candidatos potenciales de los Balcanes Occidentales.

3.2. Incidencia estimada en los gastos

3.2.1. Síntesis de la incidencia estimada en los gastos

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual:	**Número**	

			Año N[56] =2014	Año **N + 1**	Año **N + 2**	Año **N + 3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			**TOTAL**
• Créditos de operaciones										
Número de línea presupuestaria	Compromisos	(1)								
	Pagos	(2)								
Número de línea presupuestaria	Compromisos	(1a)								
	Pagos	(2a)								
Créditos de carácter administrativo financiados mediante la dotación de programas específicos[57]										
Número de línea presupuestaria		(3)								
TOTAL de los créditos para la DG	Compromisos	=1+1a +3								
	Pagos	=2+2a +3								

[56] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa.

[57] Asistencia técnica y/o administrativa y gastos de apoyo a la ejecución de programas y/o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

• TOTAL de los créditos de operaciones	Compromisos	(4)								
	Pagos	(5)								
• TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos		(6)								
TOTAL de los créditos para la RÚBRICA 3 del marco financiero plurianual	Compromisos	=4+ 6								
	Pagos	=5+ 6								

Si la propuesta/iniciativa afecta a más de una rúbrica:

• TOTAL de los créditos de operaciones	Compromisos	(4)								
	Pagos	(5)								
• TOTAL de los créditos de carácter administrativo financiados mediante la dotación de programas específicos		(6)								
TOTAL de los créditos para las RÚBRICAS 1 a 4 del marco financiero plurianual (Importe de referencia)	Compromisos	=4+ 6								
	Pagos	=5+ 6								

Rúbrica del marco financiero plurianual:	**5**	«Gastos administrativos»

En millones EUR (al tercer decimal)

	Año **N =** **2014**	Año **2015**	Año 2016	Año 2017	Año 2018	Año 2019	Año 2020	**TOTAL**
DG: JUST								

• Recursos humanos		2,922	2,922	2,922	2,922	2,922	2,922	2,922	**20,454**
• Otros gastos administrativos		0,555	0,555	0,555	0,555	0,555	0,555	0,555	**3,885**
TOTAL DG JUST		**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

TOTAL de los créditos para la RÚBRICA 5 del marco financiero plurianual	(Total créditos = Total pagos)	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

En millones EUR (al tercer decimal)

		Año **N**[58]	Año **N + 1**	Año **N + 2**	Año **N + 3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			**TOTAL**
TOTAL de los créditos para las RÚBRICAS 1 a 5 del marco financiero plurianual	Compromisos	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**
	Pagos	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

[58] El año N es el año de comienzo de la ejecución de la propuesta/iniciativa.

*3.2.2. **Incidencia estimada en los créditos de operaciones***

– ☑ La propuesta/iniciativa no exige la utilización de créditos de operaciones

Un alto nivel de protección de los datos personales es también uno de los objetivos del Programa de Derechos y Ciudadanía.

– ☐ La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

Créditos de compromiso en millones EUR (al tercer decimal)

Indíquense los objetivos y los resultados ⇩			Año **N = 2014**		Año **N + 1**		Año **N + 2**		Año **N + 3**		Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)						**TOTAL**	
			RESULTADOS															
	Tipo de resultado [59]	Coste medio del resultado	Número resultados	Coste	Número resultados	Coste	Número resultados	Coste	Número resultados	Coste	Número resultados	Coste	Número resultados	Coste	Número resultados	Coste	Número total de resultados	Total Coste
OBJETIVO ESPECÍFICO n° 1																		
[illegible]	[illegible]																	
Subtotal del objetivo específico nº 1																		
OBJETIVO ESPECÍFICO n° 2																		
- Resultado	Casos[61]																	

[59] Los resultados se refieren a los productos y servicios que se hayan de suministrar (p. ej.: número de intercambios de estudiantes financiados, número de km de carreteras construidos, etc.)

[60] Dictámenes, decisiones, reuniones de procedimiento del Consejo.

[61] Casos tratados en virtud del mecanismo de coherencia

Subtotal del objetivo específico nº 2																
COSTE TOTAL																

3.2.3. Incidencia estimada en los créditos administrativos

3.2.3.1. **Resumen**

– ☐ La propuesta/iniciativa no exige la utilización de créditos administrativos

– ☑ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año **N**[62] **2014**	Año **2015**	Año 2016	Año 2017	Año 2018	Año 2019	Año 2020	**TOTAL**
RÚBRICA 5 del marco financiero plurianual								
Recursos humanos	2,922	2,922	2,922	2,922	2,922	2,922	2,922	**20,454**
Otros gastos administrativos	0,555	0,555	0,555	0,555	0,555	0,555	0,555	**3,885**
Subtotal para la RÚBRICA 5 del marco financiero plurianual	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

Al margen de la RÚBRICA 5[63] **del marco financiero plurianual**								
Recursos humanos								
Otros gastos administrativos								
Subtotal Al margen de la RÚBRICA 5 del marco financiero plurianual								

TOTAL	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

62 El año N es el año de comienzo de la ejecución de la propuesta/iniciativa.

63 Asistencia técnica y/o administrativa y gastos de apoyo a la ejecución de programas y/o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

3.2.3.2. **Necesidades estimadas de recursos humanos**

– ☐ La propuesta/iniciativa no exige la utilización de recursos humanos

– ☑ La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

Estimación que debe expresarse en valores enteros (o a lo sumo, con un decimal)

		Año **2014**	Año **2015**	Año 2016	Año 2017	Año 2018	Año 2019	Año 2020
• Puestos de plantilla (funcionarios y agentes temporales)								
XX 01 01 01 (Sede y Oficinas de Representación de la Comisión)		22	22	22	22	22	22	22
XX 01 01 02 (Delegaciones)								
• Personal externo (en unidades de equivalente a jornada completa: EJC)[64]								
XX 01 02 01 (AC, INT, ENCS de la dotación global)		2	2	2	2	2	2	2
XX 01 02 02 (AC, INT, JED, AL y ENCS en las delegaciones)								
XX 01 04 yy[65]	- en la sede[66]							
	- en las delegaciones							
XX 01 05 02 (AC, INT, ENCS - Investigación indirecta)								
10 01 05 02 (AC, INT, ENCS - Investigación directa)								
Otras líneas presupuestarias (especifíquense)								
TOTAL		**24**	**24**	**24**	**24**	**24**	**24**	**24**

XX es el ámbito político o título presupuestario en cuestión.

Con la reforma, la Comisión tendrá que asumir nuevas tareas en materia de protección de las personas físicas por lo que se refiere al tratamiento de datos personales, además de las efectuadas actualmente. Las tareas adicionales se refieren principalmente a la aplicación del nuevo mecanismo de coherencia que garantizará la aplicación coherente de la legislación armonizada en materia de protección de datos, la evaluación de la adecuación de los terceros países, responsabilidad exclusiva de la Comisión, y la preparación de medidas de ejecución o actos delegados. La Comisión seguirá realizando las demás tareas actualmente a su cargo (por ejemplo, la

64 AC = agente contractual; INT = personal de empresas de trabajo temporal («intérimaires»); JED = joven experto en delegación; AL = agente local; ENCS = experto nacional en comisión de servicios.

65 Por debajo del límite de personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

66 Básicamente para los Fondos Estructurales, el Fondo Europeo Agrícola de Desarrollo Rural (FEADER) y el Fondo Europeo de Pesca (FEP).

elaboración de políticas, el control de la transposición, la sensibilización, las reclamaciones, etc.).

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, junto con cualquier dotación adicional que pudiera asignarse en caso necesario a la DG gestora en el marco del procedimiento de asignación anual y a la luz de las restricciones presupuestarias existentes.

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	Encargados del caso, responsables del funcionamiento del mecanismo de coherencia de la protección de datos para garantizar la unidad en la aplicación de las normas de protección de datos de la UE. Las tareas incluyen la investigación y el estudio de los casos presentados por las autoridades de los Estados miembros para que se adopte una decisión al respecto, la negociación con los Estados miembros y la preparación de las decisiones de la Comisión. Según la experiencia reciente, entre 5 y 10 casos al año pueden requerir la intervención del mecanismo de coherencia. El tratamiento de las solicitudes de adecuación requiere una interacción directa con el país solicitante, la gestión, en su caso, de estudios de expertos sobre las condiciones aplicadas en el país, la evaluación de dichas condiciones, la preparación de las decisiones pertinentes de la Comisión y del proceso, incluido en el seno del Comité que asiste a la Comisión y de los organismos especializados, si procede. Basándose en la experiencia adquirida, cabe prever hasta 4 solicitudes de adecuación al año. El proceso de adopción de las medidas de ejecución incluye medidas preparatorias como, por ejemplo, la elaboración de documentos, la investigación y las consultas públicas, así como la redacción del propio instrumento, la gestión del proceso de negociación en los comités pertinentes y en otros grupos y los contactos con las partes interesadas en general. En las zonas que requieren una orientación más precisa, podrían tratarse hasta tres medidas de ejecución al año. El proceso podría durar hasta 24 meses, dependiendo de la intensidad de las consultas.
Personal externo	Apoyo administrativo y de secretaría

3.2.4. Compatibilidad con el marco financiero plurianual actual

– ☐ La propuesta/iniciativa es compatible con el *próximo* marco financiero plurianual.

– ☑ La propuesta/iniciativa implicará la reprogramación de la rúbrica correspondiente del marco financiero plurianual.

El siguiente cuadro recoge los importes de los recursos financieros que el SEPD requiere anualmente para asumir las nuevas tareas de la Secretaría del Consejo Europeo de Protección de Datos y los procedimientos y herramientas conexos durante el periodo de las próximas perspectivas financieras, además de las ya incluidas en la planificación.

Año	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**

Personal etc.	1,555	1,555	1,543	1,543	1,543	1,543	1,543	10,823
Operaciones	0,850	1,500	1,900	1,900	1,500	1,200	1,400	10,250
Total	**2,405**	**3,055**	**3,443**	**3,443**	**3,043**	**2,743**	**2,943**	**21,073**

– ☐ La propuesta/iniciativa requiere la aplicación del Instrumento de Flexibilidad o la revisión del marco financiero plurianual[67].

3.2.5. ***Contribución de terceros***

– ☑La propuesta/iniciativa no prevé la cofinanciación por terceros.

– ☐La propuesta/iniciativa prevé la cofinanciación que se estima a continuación:

Créditos en millones EUR (al tercer decimal)

	Año **N**	Año **N + 1**	Año **N + 2**	Año **N + 3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)			Total
Especifíquese el organismo de cofinanciación								
TOTAL de los créditos cofinanciados								

3.3. ***Incidencia estimada en los ingresos***

– ☑ La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

– ☐ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

– ☐ en los recursos propios

– ☐ en ingresos diversos

En millones EUR (al tercer decimal)

Línea presupuestaria de ingresos:	Créditos disponibles para el ejercicio presupuestario en curso	Incidencia de la propuesta/iniciativa[68]				
		Año **N**	Año **N + 1**	Año **N + 2**	Año **N + 3**	Insértense tantas columnas como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)

[67] Véanse los puntos 19 y 24 del Acuerdo Interinstitucional.

[68] Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos tras la deducción del 25 % de los gastos de recaudación.

En el caso de los ingresos diversos asignados, especifíquese la línea o líneas presupuestarias de gasto en la(s) que repercuta(n).
Especifíquese el método de cálculo de la incidencia en los ingresos.

Anexo de la ficha financiera legislativa que acompaña a la 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.

Metodología aplicada y principales supuestos de base

Los gastos correspondientes a las nuevas tareas a realizar por el Supervisor Europeo de Protección de Datos (SEPD) derivadas de las dos propuestas se han estimado en función de los gastos de personal incurridos en la actualidad por la Comisión para tareas similares.

El SEPD asumirá la Secretaría del Consejo Europeo de Protección de Datos, que sustituye al Grupo de Trabajo del artículo 29. Según la carga de trabajo actual de la Comisión para esta tarea, son necesarios tres nuevos ETC con los correspondientes gastos administrativos y operativos. La carga de trabajo comenzará a partir de la entrada en vigor del Reglamento.

Además, el SEPD desempeñará una función en el mecanismo de coherencia con unas necesidades estimadas de 5 EJC, y en el desarrollo y utilización de un instrumento informático común para las Autoridades Nacionales de Protección de Datos que requerirá dos miembros del personal adicionales.

El siguiente cuadro detalla el cálculo del aumento en el gasto de personal requerido para los primeros siete años. Un segundo cuadro muestra el presupuesto operativo necesario. Esto se verá reflejado en la Sección IX del presupuesto de la UE (SEPD).

Tipo de coste	**Cálculo**	**Importe (en miles)**							
		2014	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**
Retribución y complementos									
- de la presidencia del SEPD		0,300	0,300	0,300	0,300	0,300	0,300	0,300	2,100
- de los funcionarios y agentes temporales	=7*0,127	0,889	0,889	0,889	0,889	0,889	0,889	0,889	6,223
- de los expertos en comisión de servicios	=1*0,073	0,073	0,073	0,073	0,073	0,073	0,073	0,073	0,511
- de los agentes contractuales	=2*0,064	0,128	0,128	0,128	0,128	0,128	0,128	0,128	0,896
Gastos vinculados a la contratación	=10*0,005	0,025	0,025	0,013	0,013	0,013	0,013	0,013	0,113
Gastos de misión		0,090	0,090	0,090	0,090	0,090	0,090	0,090	0,630
Otros gastos, formación	=10*0,005	0,050	0,050	0,050	0,050	0,050	0,050	0,050	0,350
Gastos administrativos totales		**1,555**	**1,555**	**1,543**	**1,543**	**1,543**	**1,543**	**1,543**	**10,823**

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	Responsables geográficos a cargo de la Secretaría del Consejo de Protección de Datos. Aparte del apoyo logístico, incluidas cuestiones contractuales y presupuestarias, la función incluye la preparación de los órdenes del día de las reuniones y las invitaciones a expertos, la investigación de temas incluidos en el orden del día del grupo, la gestión de los documentos relativos al trabajo del grupo, incluidos los requisitos pertinentes en materia de protección de datos, confidencialidad y acceso público. Sumados todos los subgrupos y grupos de expertos, cabe prever la organización de hasta 50 reuniones y procedimientos de toma de decisiones al año. Encargados del caso, responsables del funcionamiento del mecanismo de coherencia de la protección de datos para garantizar la unidad en la aplicación de las normas de protección de datos de la UE. Las tareas incluyen la investigación y el estudio de los casos presentados por las autoridades de los Estados miembros para que se adopte una decisión al respecto, la negociación con los Estados miembros y la preparación de las decisiones de la Comisión. Según la experiencia reciente, entre 5 y 10 casos al año pueden requerir la intervención del mecanismo de coherencia. La herramienta informática debería simplificar la interacción operativa entre las autoridades nacionales de protección de datos y los responsables de datos obligados a compartir información con las autoridades públicas. El o los miembros del personal responsables garantizarán el control de la calidad, la gestión del proyecto y el seguimiento presupuestario de los procesos informáticos para la especificación de los requisitos, la aplicación y el funcionamiento de los sistemas.
Personal externo	Apoyo administrativo y de secretaría

Gastos del SEPD relativos a tareas específicas

Indíquense los objetivos y los resultados			Año **N = 2014**		Año **N + 1**		Año **N + 2**		Año **N + 3**		Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)						**TOTAL**	
	RESULTADOS																	
⇩	Tipo de resultado[69]	Coste medio del resultado	Número de resultados	Coste	Número de resultados	Coste	Número de resultados	Coste	Número de resultados	Coste	Número resultados	Coste	Número resultados	Coste	Número resultados	Coste	Número total de resultados	Coste total
OBJETIVO ESPECÍFICO n° 1[70]			Secretaría del Consejo de PD															
- Resultado	Casos[71]	0,010	30	0,300	40	0,400	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	320	3,200
Subtotal del objetivo específico nº 1			30	0,300	40	0,400	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	320	3,200
OBJETIVO ESPECÍFICO n° 2			Mecanismo de Coherencia															
- Resultado	Expedientes[72]	0,050	5	0,250	10	0,500	10	0,500	10	0,500	8	0,400	8	0,400	8	0,400	59	2,950
Subtotal del objetivo específico nº 2			5	0,250	10	0,500	10	0,500	10	0,500	8	0,400	8	0,400	8	0,400	59	2,950
OBJETIVO ESPECÍFICO n° 3			Herramienta informática común para las Autoridades nacionales responsables de la Protección de Datos															
- Resultado	Casos[73]	0,100	3	0,300	6	0,600	9	0,900	9	0,900	6	0,600	3	0,300	5	0,500	41	4,100

69 Los resultados se refieren a los productos y servicios que se hayan de suministrar (p. ej.: número de intercambios de estudiantes financiados, número de km de carreteras construidos, etc.)

70 Como se describe en el punto 1.4.2. «Objetivo(s) específico(s)…»

71 Casos tratados en virtud del mecanismo de coherencia

72 Dictámenes, decisiones, reuniones de procedimiento del Consejo.

73 Los totales anuales con el resultado de la estimación de los esfuerzos necesarios para el desarrollo y explotación de las herramientas de TI

Subtotal del objetivo específico nº 3	3	0,300	6	0,600	9	0,900	9	0,900	6	0,600	3	0,300	5	0,500	41	4,100
COSTE TOTAL	38	0,850	56	1,500	69	1,900	69	1,900	64	1,500	61	1,200	63	1,400	420	10,250