Diario Oficial de la Unión Europea

L 119

Edición en lengua española

Legislación

59º año

4 de mayo de 2016

Sumario

[1] Texto pertinente a efectos del EEE

ES

Los actos cuyos títulos van impresos en caracteres finos son actos de gestión corriente, adoptados en el marco de la política agraria, y que tienen generalmente un período de validez limitado.

Los actos cuyos títulos van impresos en caracteres gruesos y precedidos de un asterisco son todos los demás actos.

I

(Actos legislativos)

REGLAMENTOS

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 27 de abril de 2016

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

(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,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de texto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo ([1]),

Visto el dictamen del Comité de las Regiones ([2]),

De conformidad con el procedimiento legislativo ordinario ([3]),

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 («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende 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 las personas físicas.

(3) La Directiva 95/46/CE del Parlamento Europeo y del Consejo ([4]) trata de 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.

([1]) DO C 229 de 31.7.2012, p. 90.
([2]) DO C 391 de 18.12.2012, p. 127.
([3]) Posición del Parlamento Europeo de 12 de marzo de 2014 (pendiente de publicación en el Diario Oficial) y posición del Consejo en primera lectura de 8 de abril de 2016 (pendiente de publicación en el Diario Oficial). Posición del Parlamento Europeo de 14 de abril de 2016.
([4]) 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) El tratamiento de datos personales debe estar concebido para servir a la humanidad. 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 las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, 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, y la diversidad cultural, religiosa y lingüística.

(5) La integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos de datos personales. En toda la Unión se ha incrementado el intercambio de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas. El Derecho de la Unión insta a las autoridades nacionales de los Estados miembros a que cooperen e intercambien datos personales a fin de poder cumplir sus funciones o desempeñar otras por cuenta de una autoridad de otro Estado miembro.

(6) La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar 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, y ha de facilitar aún más la libre circulación de datos personales 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.

(7) Estos avances requieren 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. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

(8) En los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento.

(9) Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular en relación con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección de los datos de carácter personal, en lo que respecta al tratamiento de 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 las funciones 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.

(10) Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, 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 que la aplicación 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 sea coherente y homogénea. En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento. Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito.

(11) La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes.

(12) El artículo 16, apartado 2, del TFUE encomienda 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.

(13) Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles 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 entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Con objeto de tener en cuenta la situación específica de las microempresas y las pequeñas y medianas empresas, el presente Reglamento incluye una serie de excepciones en materia de llevanza de registros para organizaciones con menos de 250 empleados. Además, alienta a las instituciones y órganos de la Unión y a los Estados miembros y a sus autoridades de control a tener en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas en la aplicación del presente Reglamento. El concepto de microempresas y pequeñas y medianas empresas debe extraerse del artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión ([1]).

(14) La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales 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.

(15) A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento.

(16) El presente Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

(17) El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo ([2]) se aplica al tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal deben adaptarse a los principios y normas establecidos en el presente Reglamento y aplicarse a la luz del mismo. A fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión, una vez adoptado el presente Reglamento deben introducirse las adaptaciones necesarias del Reglamento (CE) n.º 45/2001, con el fin de que pueda aplicarse al mismo tiempo que el presente Reglamento.

(18) El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad

([1]) Recomendación de la Comisión de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas [C(2003) 1422] (DO L 124 de 20.5.2003, p. 36).

([2]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

(19) 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 de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El presente Reglamento no debe, por lo tanto, aplicarse a las actividades de tratamiento destinadas a tales fines. No obstante, los datos personales tratados por las autoridades públicas en aplicación del presente Reglamento deben, si se destinan a tales fines, regirse por un acto jurídico de la Unión más específico, concretamente la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo ([1]). Los Estados miembros pueden encomendar a las autoridades competentes, tal como se definen en la Directiva (UE) 2016/680, funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del presente Reglamento.

En lo que respecta al tratamiento de datos personales por parte de dichas autoridades competentes con fines que entren en el ámbito de aplicación del presente Reglamento, los Estados miembros deben tener la posibilidad de mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del presente Reglamento. Tales disposiciones pueden establecer de forma más precisa requisitos concretos para el tratamiento de datos personales con otros fines por parte de dichas autoridades competentes, tomando en consideración la estructura constitucional, organizativa y administrativa del Estado miembro en cuestión. Cuando el tratamiento de datos personales por organismos privados entre en el ámbito de aplicación del presente Reglamento, este debe disponer que los Estados miembros puedan, en condiciones específicas, limitar conforme a Derecho determinadas obligaciones y derechos siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención. Esto se aplica, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o de las actividades de los laboratorios de policía científica.

(20) Aunque el presente Reglamento se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales, en virtud del Derecho de la Unión o de los Estados miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento en relación con el tratamiento de datos personales por los tribunales y otras autoridades judiciales. A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos.

(21) El presente Reglamento debe entenderse sin perjuicio de la aplicación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo ([2]), en particular de las normas en materia de responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15. El objetivo de dicha Directiva es contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros.

(22) 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 que el tratamiento tenga lugar en la Unión. Un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto.

([1]) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (véase la página 89 del presente Diario Oficial).

([2]) 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).

(23) 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 interesados que residen en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

(24) El tratamiento de datos personales de los interesados que residen en la Unión por un responsable o encargado no establecido en la Unión debe ser también objeto del presente Reglamento cuando esté relacionado con la observación del comportamiento de dichos interesados en la medida en que este comportamiento tenga lugar en la Unión. Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

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

(26) Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

(27) El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas.

(28) La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.

(29) Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas.

(30) Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.

(31) Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento.

(32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, 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, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

(33) Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.

(34) Debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

(35) Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo ([1]); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

(36) El establecimiento principal de un responsable del tratamiento en la Unión debe ser el lugar de su administración central en la Unión, salvo que las decisiones relativas a los fines y medios del tratamiento de los datos personales se tomen en otro establecimiento del responsable en la Unión, en cuyo caso, ese otro establecimiento debe

([1]) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

considerarse el establecimiento principal. El establecimiento principal de un responsable 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 y medios del tratamiento a través de modalidades estables. Dicho criterio no debe depender de si el tratamiento de los datos personales se realiza 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, establecimiento principal y no son, por lo tanto, criterios determinantes de un establecimiento principal. El establecimiento principal del encargado del tratamiento debe ser el lugar de su administración central en la Unión o, si careciese de administración central en la Unión, el lugar en el que se llevan a cabo las principales actividades de tratamiento en la Unión. En los casos que impliquen tanto al responsable como al encargado, la autoridad de control principal competente debe seguir siendo la autoridad de control del Estado miembro en el que el responsable tenga su establecimiento principal, pero la autoridad de control del encargado debe considerarse autoridad de control interesada y participar en el procedimiento de cooperación establecido en el presente Reglamento. En cualquier caso, las autoridades de control del Estado miembro o los Estados miembros en los que el encargado tenga uno o varios establecimientos no deben considerarse autoridades de control interesadas cuando el proyecto de decisión afecte únicamente al responsable. Cuando el tratamiento lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine otra empresa.

(37) Un grupo empresarial debe estar constituido por una empresa que ejerce el control y las empresas controladas, debiendo ser la empresa que ejerce el control la que pueda ejercer una influencia dominante en las otras empresas, por razones, por ejemplo, de propiedad, participación financiera, normas por las que se rige, o poder de hacer cumplir las normas de protección de datos personales. Una empresa que controle el tratamiento de los datos personales en las empresas que estén afiliadas debe considerarse, junto con dichas empresas, «grupo empresarial».

(38) Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.

(39) Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

(40) Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de

otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.

(41) Cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate. Sin embargo, dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia») y del Tribunal Europeo de Derechos Humanos.

(42) Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo ([1]), debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

(43) Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento.

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

(45) Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional.

(46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente

([1]) Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95 de 21.4.1993, p. 29).

deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

(47) El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.

(48) Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. Los principios generales aplicables a la transmisión de datos personales, dentro de un grupo empresarial, a una empresa situada en un país tercero no se ven afectados.

(49) Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

(50) El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado

basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. 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 y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable. Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto.

(51) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de 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.

(52) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública 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 con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

(53) Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto

profesional. El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos.

(54) El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo ([1]), es decir, todos los elementos relacionados con la salud, concretamente 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 relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.

(55) Se realiza además por razones de interés público el tratamiento de datos personales por las autoridades públicas con el fin de alcanzar los objetivos, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente.

(56) Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas.

(57) Si los datos personales tratados por un responsable no le permiten identificar a una persona física, el responsable no debe estar obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir cualquier disposición del presente Reglamento. No obstante, el responsable del tratamiento no debe negarse a recibir información adicional facilitada por el interesado a fin de respaldarle en el ejercicio de sus derechos. La identificación debe incluir la identificación digital de un interesado, por ejemplo mediante un mecanismo de autenticación, como las mismas credenciales, empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el responsable.

(58) El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

(59) Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas.

([1]) Reglamento (CE) n.º 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 (DO L 354 de 31.12.2008, p. 70).

(60) Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente.

(61) Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general.

(62) Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas.

(63) Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento. Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. 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 programas informáticos. No obstante, estas consideraciones no deben tener como resultado la negativa a prestar toda la información al interesado. Si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud.

(64) 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. El responsable no debe conservar datos personales con el único propósito de poder responder a posibles solicitudes.

(65) Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su

consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

(66) A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

(67) Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

(68) Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato. Por su propia naturaleza, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable. El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles. Cuando un conjunto de datos personales determinado concierna a más de un interesado, el derecho a recibir tales datos se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento. Por otra parte, ese derecho no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el presente Reglamento, y en particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato. El interesado debe tener derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible.

(69) En los casos en que los datos personales puedan ser tratados lícitamente porque el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o por motivos de intereses legítimos del responsable o de un tercero, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado.

(70) Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información.

(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor.

A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas.

(72) La elaboración de perfiles está sujeta a las normas del presente Reglamento que rigen el tratamiento de datos personales, como los fundamentos jurídicos del tratamiento o los principios de la protección de datos. El Comité Europeo de Protección de Datos establecido por el presente Reglamento (en lo sucesivo, el «Comité») debe tener la posibilidad de formular orientaciones en este contexto.

(73) El Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfiles, así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios. Dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

(74) Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

(76) La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

(77) Se podrían proporcionar directrices para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento, especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo, que revistan, en particular, la forma de códigos de conducta aprobados, certificaciones aprobadas, directrices dadas por el Comité o indicaciones proporcionadas por un delegado de protección de datos. El Comité también puede emitir directrices sobre operaciones de tratamiento que se considere improbable supongan un alto riesgo para los derechos y libertades de las personas físicas, e indicar qué medidas pueden ser suficientes en dichos casos para afrontar el riesgo en cuestión.

(78) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

(79) La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.

(80) El responsable o el encargado del tratamiento no establecido en la Unión que esté tratando datos personales de interesados que residan en la Unión y cuyas actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere un pago por parte de estos, o con el control de su comportamiento en la medida en que este tenga lugar en la Unión, debe designar a un representante, a menos que el tratamiento sea ocasional, no incluya el tratamiento a gran escala de categorías especiales de datos personales o el tratamiento de datos personales relativos a condenas e infracciones penales, y sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, vista la naturaleza, el

contexto, el ámbito y los fines del tratamiento, o si el responsable del tratamiento es una autoridad u organismo público. El representante debe actuar por cuenta del responsable o el encargado y puede ser contactado por cualquier autoridad de control. El representante debe ser designado expresamente por mandato escrito del responsable o del encargado para que actúe en su nombre con respecto a las obligaciones que les incumben en virtud del presente Reglamento. La designación de dicho representante no afecta a la responsabilidad del responsable o del encargado en virtud del presente Reglamento. Dicho representante debe desempeñar sus funciones conforme al mandato recibido del responsable o del encargado, incluida la cooperación con las autoridades de control competentes en relación con cualquier medida que se tome para garantizar el cumplimiento del presente Reglamento. El representante designado debe estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado.

(81) Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos.

(82) Para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad. Todos los responsables y encargados están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento.

(83) A fin 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, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

(84) A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona

física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

(87) Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento.

(88) Al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, hay que tener debidamente en cuenta las circunstancias de tal violación, inclusive 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 las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales.

(89) La Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control. Pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales. Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.

(90) En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento.

(91) Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hace más difícil para los interesados el ejercicio de sus

derechos. La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas. También es necesaria una evaluación de impacto relativa a la protección de datos para el control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos o para cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados, en particular porque impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato, o porque se efectúe sistemáticamente a gran escala. El tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud o abogado. En estos casos, la evaluación de impacto de la protección de datos no debe ser obligatoria.

(92) Hay circunstancias en las que puede ser razonable y económico que una evaluación de impacto relativa a la protección de datos abarque más de un único proyecto, por ejemplo, en el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyecten introducir una aplicación o un entorno de tratamiento común en un sector o segmento empresarial o para una actividad horizontal de uso generalizado.

(93) Los Estados miembros, al adoptar el Derecho en el que se basa el desempeño de las funciones de la autoridad pública o el organismo público y que regula la operación o el conjunto de operaciones de tratamiento en cuestión, pueden considerar necesario llevar a cabo dicha evaluación con carácter previo a las actividades de tratamiento.

(94) Debe consultarse a la autoridad de control antes de iniciar las actividades de tratamiento si una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación. Existe la probabilidad de que ese alto riesgo se deba a determinados tipos de tratamiento y al alcance y frecuencia de este, lo que también puede ocasionar daños y perjuicios o una injerencia en los derechos y libertades de la persona física. La autoridad de control debe responder a la solicitud de consulta dentro de un plazo determinado. Sin embargo, la ausencia de respuesta de la autoridad de control dentro de dicho plazo no debe obstar a cualquier intervención de dicha autoridad basada en las funciones y poderes que le atribuye el presente Reglamento, incluido el poder de prohibir operaciones de tratamiento. Como parte de dicho proceso de consulta, se puede presentar a la autoridad de control el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas.

(95) El encargado del tratamiento debe asistir al responsable cuando sea necesario y a petición suya, a fin de asegurar que se cumplen las obligaciones que se derivan de la realización de las evaluaciones de impacto relativas a la protección de datos y de la consulta previa a la autoridad de control.

(96) Deben llevarse también a cabo consultas con la autoridad de control en el curso de la tramitación de una medida legislativa o reglamentaria que establezca el tratamiento de datos personales, a fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, en particular, de mitigar el riesgo que implique el tratamiento para el interesado.

(97) Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales

como actividades auxiliares. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente.

(98) Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados 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 y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento.

(99) Al elaborar un código de conducta, o al modificar o ampliar dicho código, las asociaciones y otros organismos que representan a categorías de responsables o encargados deben consultar a las partes interesadas, incluidos los interesados cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas en respuesta a dichas consultas.

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

(101) Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.

(102) El presente Reglamento se entiende sin perjuicio de los acuerdos internacionales celebrados entre la Unión y terceros países que regulan la transferencia de datos personales, incluidas las oportunas garantías para los interesados. Los Estados miembros pueden celebrar acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al presente Reglamento ni a ninguna otra disposición del Derecho de la Unión e incluyan un nivel adecuado de protección de los derechos fundamentales de los interesados.

(103) La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u organización internacional que se considera ofrece tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización. La Comisión también puede decidir revocar esa decisión, previo aviso y completa declaración motivada al tercer país u organización internacional.

(104) 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, o de un territorio o un sector específico de un tercer país, debe tener en cuenta de qué manera respeta un determinado tercer país respeta el Estado de Derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos y su Derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal. En la adopción de una decisión de adecuación con respecto a un territorio o un sector específico de un tercer país se deben tener en cuenta criterios claros y objetivos, como las actividades concretas de tratamiento y el alcance de las normas jurídicas aplicables y la legislación vigente en el

tercer país. El tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas.

(105) Aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión debe tener en cuenta las obligaciones resultantes de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones. En particular, debe tenerse en cuenta la adhesión del país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo adicional. La Comisión debe consultar al Comité al evaluar el nivel de protección existente en terceros países u organizaciones internacionales.

(106) La Comisión debe supervisar la aplicación de las decisiones sobre el nivel de protección en un país tercero, un territorio o un sector específico de un país tercero, o una organización internacional, y la aplicación las decisiones adoptadas sobre la base del artículo 25, apartado 6, o el artículo 26, apartado 4, de la Directiva 95/46/CE. En sus decisiones de adecuación, la Comisión debe establecer un mecanismo para la revisión periódica de su aplicación. Dicha revisión periódica debe realizarse en colaboración con el tercer país u organización internacional de que se trate y tener en cuenta todos los cambios en la materia que se produzcan en dicho tercer país u organización internacional. A efectos de la supervisión y realización de las revisiones periódicas, la Comisión debe tomar en consideración las opiniones y conclusiones del Parlamento Europeo y del Consejo, así como de otros organismos y fuentes pertinentes. La Comisión debe evaluar, en un plazo razonable, la aplicación de dichas decisiones e informar de cualquier conclusión pertinente al Comité que, en el sentido del Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([1]), establece el presente Reglamento, y al Parlamento Europeo y el Consejo.

(107) La Comisión puede reconocer que un tercer país, un territorio o sector específico en un tercer país, o una organización internacional ya no garantiza un nivel de protección de datos adecuado. En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país u organización internacional, salvo que se cumplan los requisitos del presente Reglamento relativos a las transferencias basadas en garantías adecuadas, incluidas las normas corporativas vinculantes, y a las excepciones aplicadas a situaciones específicas. En ese caso, debe establecerse la celebración de consultas entre la Comisión y esos terceros países u organizaciones internacionales. La Comisión debe informar en tiempo oportuno al tercer país u organización internacional de las razones y entablar consultas a fin de subsanar la situación.

(108) En ausencia de una decisión por la que se constate la adecuación 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 garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto. Las transferencias también pueden realizarlas autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes se debe recabar la autorización de la autoridad de control competente.

(109) La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe obstar a que los responsables o encargados

([1]) Reglamento (UE) n.º 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).

incluyan las cláusulas tipo de protección de datos en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control, ni mermen los derechos o las libertades fundamentales de los interesados. Se debe alentar a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos.

(110) Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal.

(111) Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, de mediar el consentimiento explícito del interesado, si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores. También se debe establecer la posibilidad de realizar transferencias cuando así lo requieran razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros, o cuando la transferencia se haga a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo. En este último caso la transferencia no debe afectar a la totalidad de los datos personales o de las categorías de datos incluidos en el registro y, cuando el registro esté destinado a su consulta 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, teniendo plenamente en cuenta los intereses y los derechos fundamentales del interesado.

(112) Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento. En ausencia de una decisión de adecuación, el Derecho de la Unión o de los Estados miembros puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional. Los Estados miembros deben notificar esas disposiciones a la Comisión. Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados.

(113) Las transferencias que pueden calificarse de no repetitivas y sólo se refieren a un número limitado de interesados, también han de ser posibles en caso de servir a intereses legítimos imperiosos del responsable del tratamiento, si no prevalecen sobre ellos los intereses o los derechos y libertades del interesado y el responsable ha evaluado todas las circunstancias concurrentes en la transferencia de datos. El responsable debe prestar especial atención a la naturaleza de los datos personales, 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 ofrecer, garantías apropiadas para proteger los derechos fundamentales y las libertades de las personas físicas con respecto al tratamiento de sus datos personales. Dichas transferencias sólo deben ser posibles en casos aislados, cuando ninguno de los otros motivos para la transferencia sean aplicables. Las legítimas expectativas de la sociedad en un aumento del conocimiento se deben tener en cuenta para fines de investigación científica o histórica o fines estadísticos. El responsable debe informar de la transferencia a la autoridad de control y al interesado.

(114) En cualquier caso, cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de la protección de datos en un tercer país, el responsable o el encargado del tratamiento deben arbitrar soluciones que garanticen a los interesados derechos exigibles y efectivos con respecto al tratamiento de sus datos en la Unión, una vez transferidos estos, de forma que sigan beneficiándose de derechos fundamentales y garantías.

(115) Algunos países terceros adoptan leyes, reglamentaciones y otros actos jurídicos con los que se pretende regular directamente las actividades de tratamiento de personas físicas y jurídicas bajo jurisdicción de los Estados miembros. Esto puede incluir sentencias de órganos jurisdiccionales o decisiones de autoridades administrativas de terceros países que obliguen a un responsable o un encargado del tratamiento a transferir o comunicar datos personales, y que no se basen en un acuerdo internacional, como un tratado de asistencia judicial mutua, en vigor entre el tercer país requirente y la Unión o un Estado miembro. La aplicación extraterritorial de dichas leyes, reglamentaciones y otros actos jurídicos puede ser contraria al Derecho internacional e impedir la protección de las personas físicas garantizada en la Unión en virtud del presente Reglamento. Las transferencias solo deben autorizarse cuando se cumplan las condiciones del presente Reglamento relativas a las transferencias a terceros países. Tal puede ser el caso, entre otros, cuando la comunicación sea necesaria por una razón importante de interés público reconocida por el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento.

(116) Cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión 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 o comunicación ilícitas 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 correctivos insuficientes, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. Por consiguiente, es necesario fomentar una cooperación más estrecha entre las autoridades de control encargadas de la protección de datos para ayudarlas a intercambiar información y a llevar a cabo investigaciones con sus homólogos internacionales. A fin de desarrollar mecanismos de cooperación internacional que faciliten y proporcionen asistencia internacional mutua en la ejecución de legislación en materia de protección de datos personales, la Comisión y las autoridades de control deben intercambiar información y cooperar en actividades relativas al ejercicio de sus competencias con las autoridades competentes de terceros países, sobre la base de la reciprocidad y de conformidad con el presente Reglamento.

(117) El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.

(118) La independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial.

(119) Si un Estado miembro establece varias autoridades de control, debe disponer por ley mecanismos que garanticen la participación efectiva de dichas autoridades de control en el mecanismo de coherencia. Tal Estado miembro debe, en particular, designar a la autoridad de control que actuará como punto de contacto único de cara a la participación efectiva de dichas autoridades en el citado mecanismo, garantizando así una cooperación rápida y fluida con otras autoridades de control, el Comité y la Comisión.

(120) Todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus funciones, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión. Cada autoridad de control debe disponer de un presupuesto anual público propio, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

(121) Las condiciones generales aplicables al miembro o los miembros de la autoridad de control deben establecerse por ley en cada Estado miembro y disponer, en particular, que dichos miembros han de ser nombrados, por un procedimiento transparente, por el Parlamento, el Gobierno o el jefe de Estado del Estado miembro, a propuesta del Gobierno, de un miembro del Gobierno o del Parlamento o una de sus cámaras, o por un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros. A fin de garantizar la independencia de la autoridad de control, sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones y no participar, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada. La autoridad de control debe tener su propio personal, seleccionado por esta o por un organismo independiente establecido por el Derecho de los Estados miembros, que esté subordinado exclusivamente al miembro o los miembros de la autoridad de control.

(122) Cada autoridad de control debe ser competente, en el territorio de su Estado miembro, para ejercer los poderes y desempeñar las funciones que se le confieran de conformidad con el presente Reglamento. Lo anterior debe

abarcar, en particular, el tratamiento en el contexto de las actividades de un establecimiento del responsable o del encargado en el territorio de su Estado miembro, el tratamiento de datos personales realizado por autoridades públicas o por organismos privados que actúen en interés público, el tratamiento que afecte a interesados en su territorio, o el tratamiento realizado por un responsable o un encargado que no esté establecido en la Unión cuando sus destinatarios sean interesados residentes en su territorio. Debe incluirse el examen de reclamaciones presentadas por un interesado, la realización de investigaciones sobre la aplicación del presente Reglamento y el fomento de la sensibilización del público acerca de los riesgos, las normas, las garantías y los derechos en relación con el tratamiento de datos personales.

(123) A fin de proteger a las personas físicas con respecto al tratamiento de sus datos personales y de facilitar la libre circulación de los datos personales en el mercado interior, las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión. A tal efecto, las autoridades de control deben cooperar entre ellas y con la Comisión, sin necesidad de acuerdo alguno entre Estados miembros sobre la prestación de asistencia mutua ni sobre dicha cooperación.

(124) Si el tratamiento de datos personales se realiza en el contexto de las actividades de un establecimiento de un responsable o un encargado en la Unión y el responsable o el encargado está establecido en más de un Estado miembro, o si el tratamiento en el contexto de las actividades de un único establecimiento de un responsable o un encargado en la Unión afecta o es probable que afecte sustancialmente a interesados en más de un Estado miembro, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado debe actuar como autoridad principal. Dicha autoridad debe cooperar con las demás autoridades interesadas, ya sea porque el responsable o el encargado tenga un establecimiento en el territorio de su Estado miembro, porque afecte sustancialmente a interesados que residen en su territorio, o porque se haya presentado una reclamación ante ellas. Asimismo, cuando un interesado que no resida en ese Estado miembro haya presentado una reclamación, la autoridad de control ante la que se haya presentado esta también debe ser autoridad de control interesada. En el marco de sus funciones de formulación de directrices sobre cualquier cuestión relacionada con la aplicación del presente Reglamento, el Comité debe estar facultado para formular directrices, en particular sobre los criterios que han de tenerse en cuenta para determinar si el tratamiento en cuestión afecta sustancialmente a interesados de más de un Estado miembro y sobre lo que constituya una objeción pertinente y motivada.

(125) La autoridad principal debe ser competente para adoptar decisiones vinculantes relativas a las medidas de aplicación de los poderes conferidos con arreglo al presente Reglamento. En su calidad de autoridad principal, la autoridad de control debe implicar estrechamente y coordinar a las autoridades de control interesadas en el proceso de toma de decisiones. En los casos en los que la decisión consista en rechazar total o parcialmente la reclamación del interesado, esa decisión debe ser adoptada por la autoridad de control ante la que se haya presentado la reclamación.

(126) La decisión debe ser acordada conjuntamente por la autoridad de control principal y las autoridades de control interesadas y debe dirigirse al establecimiento principal o único del responsable o del encargado del tratamiento y ser vinculante para ambos. El responsable o el encargado deben tomar las medidas necesarias para garantizar el cumplimiento del presente Reglamento y la aplicación de la decisión notificada por la autoridad de control principal al establecimiento principal del responsable o del encargado en lo que se refiere a las actividades de tratamiento en la Unión.

(127) Cada autoridad de control que no actúa como autoridad principal debe ser competente para tratar asuntos locales en los que, si bien el responsable o el encargado del tratamiento está establecido en más de un Estado miembro, el objeto del tratamiento específico se refiere exclusivamente al tratamiento efectuado en un único Estado miembro y afecta exclusivamente a interesados de ese único Estado miembro, por ejemplo cuando el tratamiento tiene como objeto datos personales de empleados en el contexto específico de empleo de un Estado miembro. En tales casos, la autoridad de control debe informar sin dilación al respecto a la autoridad de control principal. Una vez informada, la autoridad de control principal debe decidir si tratará el asunto de acuerdo con la disposición aplicable a la cooperación entre la autoridad de control principal y otras autoridades de control interesadas («mecanismo de ventanilla única»), o si lo debe tratar localmente la autoridad de control que le haya informado. Al decidir si trata el asunto, la autoridad de control principal debe considerar si existe un establecimiento del responsable o del encargado en el Estado miembro de la autoridad de control que le haya informado, con el fin de garantizar la ejecución efectiva de la decisión respecto del responsable o encargado del tratamiento. Si la autoridad de control principal decide tratar el asunto, se debe ofrecer a la autoridad de control informante la

posibilidad de presentar un proyecto de decisión, que la autoridad de control principal ha de tener en cuenta en la mayor medida posible al preparar su proyecto de decisión al amparo del mecanismo de ventanilla única.

(128) Las normas sobre la autoridad de control principal y el mecanismo de ventanilla única no deben aplicarse cuando el tratamiento sea realizado por autoridades públicas u organismos privados en interés público. En tales casos, la única autoridad de control competente para ejercer los poderes conferidos con arreglo al presente Reglamento debe ser la autoridad de control del Estado miembro en el que estén establecidos la autoridad pública o el organismo privado.

(129) Para garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las competencias de las autoridades encargadas de la persecución de los delitos con arreglo al Derecho de los Estados miembros para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y ejercitar acciones judiciales. Dichos poderes deben incluir también el poder de imponer una limitación temporal o definitiva al tratamiento, incluida su prohibición. Los Estados miembros pueden especificar otras funciones relacionadas con la protección de datos personales con arreglo al presente Reglamento. Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto, respetar el derecho de todas las personas a ser oídas antes de que se adopte cualquier medida que las afecte negativamente y evitar costes superfluos y molestias excesivas para las personas afectadas. Los poderes de investigación en lo que se refiere al acceso a instalaciones deben ejercerse de conformidad con los requisitos específicos del Derecho procesal de los Estados miembros, como el de la autorización judicial previa. Toda medida jurídicamente vinculante de la autoridad de control debe constar por escrito, ser clara e inequívoca, indicar la autoridad de control que dictó la medida y la fecha en que se dictó, llevar la firma del director o de un miembro de la autoridad de control autorizado por este, especificar los motivos de la medida y mencionar el derecho a la tutela judicial efectiva. Esto no debe obstar a que se impongan requisitos adicionales con arreglo al Derecho procesal de los Estados miembros. La adopción de una decisión jurídicamente vinculante implica que puede ser objeto de control judicial en el Estado miembro de la autoridad de control que adoptó la decisión.

(130) Cuando la autoridad de control ante la cual se haya presentado la reclamación no sea la autoridad de control principal, esta última debe cooperar estrechamente con la primera con arreglo a las disposiciones sobre cooperación y coherencia establecidas en el presente Reglamento. En tales casos, la autoridad de control principal, al tomar medidas concebidas para producir efectos jurídicos, incluida la imposición de multas administrativas, debe tener en cuenta en la mayor medida posible la opinión de la autoridad de control ante la cual se haya presentado la reclamación y la cual debe seguir siendo competente para realizar cualquier investigación en el territorio de su propio Estado miembro en enlace con la autoridad de control competente.

(131) En casos en los que otra autoridad de control deba actuar como autoridad de control principal para las actividades de tratamiento del responsable o del encargado pero el objeto concreto de una reclamación o la posible infracción afecta únicamente a las actividades de tratamiento del responsable o del encargado en el Estado miembro en el que se haya presentado la reclamación o detectado la posible infracción y el asunto no afecta sustancialmente ni es probable que afecte sustancialmente a interesados de otros Estados miembros, la autoridad de control que reciba una reclamación o que detecte situaciones que conlleven posibles infracciones del presente Reglamento o reciba de otra manera información sobre estas debe tratar de llegar a un arreglo amistoso con el responsable del tratamiento y, si no prospera, ejercer todos sus poderes. En lo anterior se debe incluir el tratamiento específico realizado en el territorio del Estado miembro de la autoridad de control o con respecto a interesados en el territorio de dicho Estado miembro; el tratamiento efectuado en el contexto de una oferta de bienes o servicios destinada específicamente a interesados en el territorio del Estado miembro de la autoridad de control; o el tratamiento que deba evaluarse teniendo en cuenta las obligaciones legales pertinentes en virtud del Derecho de los Estados miembros.

(132) Entre las actividades de sensibilización del público por parte de las autoridades de control deben incluirse medidas específicas dirigidas a los responsables y los encargados del tratamiento, incluidas las microempresas y las pequeñas y medianas empresas, así como las personas físicas, en particular en el contexto educativo.

(133) Las autoridades de control se deben ayudar una a otra en el desempeño de sus funciones y prestar asistencia mutua, con el fin de garantizar la aplicación y ejecución coherentes del presente Reglamento en el mercado interior. Una autoridad de control que solicite asistencia mutua puede adoptar una medida provisional si no recibe respuesta a su solicitud de asistencia en el plazo de un mes a partir de su recepción por la otra autoridad de control.

(134) Cada autoridad de control debe participar, cuando proceda, en operaciones conjuntas con otras autoridades de control. La autoridad de control a la que se solicite ayuda debe tener la obligación de responder a la solicitud en un plazo de tiempo determinado.

(135) A fin de garantizar la aplicación coherente del presente Reglamento en toda la Unión, debe establecerse un mecanismo de coherencia para la cooperación entre las autoridades de control. Este mecanismo debe aplicarse en particular cuando una autoridad de control prevea adoptar una medida dirigida a producir efectos jurídicos en lo que se refiere a operaciones de tratamiento que afecten sustancialmente a un número significativo de interesados en varios Estados miembros. También debe aplicarse cuando cualquier autoridad de control interesada o la Comisión soliciten que dicho asunto se trate al amparo del mecanismo de coherencia. Dicho mecanismo debe entenderse sin perjuicio de cualesquiera medidas que la Comisión pueda adoptar en el ejercicio de sus poderes con arreglo a los Tratados.

(136) En aplicación del mecanismo de coherencia, el Comité debe, en un plazo determinado, emitir un dictamen, si así lo decide una mayoría de sus miembros o si así lo solicita cualquier autoridad de control interesada o la Comisión. El Comité también debe estar facultado para adoptar decisiones jurídicamente vinculantes en caso de diferencias entre autoridades de control. A tal efecto debe dictar, en principio por mayoría de dos tercios de sus miembros, decisiones jurídicamente vinculantes en casos claramente especificados en los que exista conflicto de opiniones entre las autoridades de control, en particular en el mecanismo de cooperación entre la autoridad de control principal y las autoridades de control interesadas sobre el fondo del asunto, especialmente en caso de infracción del presente Reglamento.

(137) La necesidad urgente de actuar puede obedecer a la necesidad de proteger los derechos y libertades de los interesados, en particular cuando exista el riesgo de que pueda verse considerablemente obstaculizado el reconocimiento de alguno de sus derechos. Por lo tanto, una autoridad de control debe poder adoptar en su territorio medidas provisionales, debidamente justificadas, con un plazo de validez determinado no superior a tres meses.

(138) La aplicación de tal mecanismo debe ser una condición para la licitud de una medida de una autoridad de control destinada a producir efectos jurídicos, en aquellos casos en los que su aplicación sea obligatoria. En otros casos de relevancia transfronteriza, la autoridad de control principal y las autoridades de control interesadas deben aplicar entre sí el mecanismo de cooperación, y las autoridades de control interesadas pueden prestarse asistencia mutua y realizar entre sí operaciones conjuntas, sobre una base bilateral o multilateral, sin tener que aplicarlo.

(139) A fin de fomentar la aplicación coherente del presente Reglamento, el Comité debe constituirse como organismo independiente de la Unión. Para cumplir sus objetivos, el Comité debe tener personalidad jurídica. Su presidente debe ostentar su representación. El Comité 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 el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de Protección de Datos, o por sus respectivos representantes. La Comisión debe participar en las actividades del Comité sin derecho a voto y se deben reconocer derechos de voto específicos al Supervisor Europeo de Protección de Datos. El Comité debe contribuir a la aplicación coherente del presente Reglamento en toda la Unión, entre otras cosas asesorando a la Comisión, en particular sobre el nivel de protección en terceros países u organizaciones internacionales, y fomentando la cooperación de las autoridades de control en toda la Unión. El Comité debe actuar con independencia en el cumplimiento de sus funciones.

(140) El Comité debe contar con una secretaría, a cargo el Supervisor Europeo de Protección de Datos. El personal del Supervisor Europeo de Protección de Datos que participe en la realización de las funciones conferidas al Comité por el presente Reglamento debe desempeñar sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité y responder ante él.

(141) Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y derecho a la tutela judicial efectiva de conformidad

con el artículo 47 de la Carta si considera que se vulneran sus derechos con arreglo al presente Reglamento o en caso de que la autoridad de control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado. La investigación a raíz de una reclamación debe llevarse a cabo, bajo control judicial, si procede en el caso concreto. La autoridad de control debe informar al interesado de la evolución y el resultado de la reclamación en un plazo razonable. Si el asunto requiere una mayor investigación o coordinación con otra autoridad de control, se debe facilitar información intermedia al interesado. Para facilitar la presentación de reclamaciones, cada autoridad de control debe adoptar medidas como el suministro de un formulario de reclamaciones, que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

(142) El interesado que considere vulnerados los derechos reconocidos por el presente Reglamento debe tener derecho a conferir mandato a una entidad, organización o asociación sin ánimo de lucro que esté constituida con arreglo al Derecho de un Estado miembro, tenga objetivos estatutarios que sean de interés público y actúe en el ámbito de la protección de los datos personales, para que presente en su nombre una reclamación ante la autoridad de control, ejerza el derecho a la tutela judicial en nombre de los interesados o, si así lo establece el Derecho del Estado miembro, ejerza el derecho a recibir una indemnización en nombre de estos. Un Estado miembro puede reconocer a tal entidad, organización o asociación el derecho a presentar en él una reclamación con independencia del mandato de un interesado y el derecho a la tutela judicial efectiva, cuando existan motivos para creer que se han vulnerado los derechos de un interesado como consecuencia de un tratamiento de datos personales que sea contrario al presente Reglamento. Esa entidad, organización o asociación no puede estar autorizada a reclamar una indemnización en nombre de un interesado al margen del mandato de este último.

(143) Toda persona física o jurídica tiene derecho a interponer ante el Tribunal de Justicia recurso de anulación de decisiones del Comité, en las condiciones establecidas en el artículo 263 del TFUE. Como destinatarias de dichas decisiones, las autoridades de control interesadas que quieran impugnarlas tienen que interponer recurso en el plazo de dos meses a partir del momento en que les fueron notificadas, de conformidad con el artículo 263 del TFUE. En caso de que las decisiones del Comité afecten directa e individualmente a un responsable, un encargado o al reclamante, estos pueden interponer recurso de anulación de dichas decisiones en el plazo de dos meses a partir de su publicación en el sitio web del Comité, de conformidad con el artículo 263 del TFUE. Sin perjuicio de lo dispuesto en el artículo 263 del TFUE, toda persona física o jurídica debe tener derecho a la tutela judicial efectiva ante el tribunal nacional competente contra las decisiones de una autoridad de control que produzcan efectos jurídicos que le afecten. Tales decisiones se refieren en particular al ejercicio de los poderes de investigación, corrección y autorización por parte de la autoridad de control o a la desestimación o rechazo de reclamaciones. No obstante, el derecho a la tutela judicial efectiva no incluye medidas adoptadas por las autoridades de control que no sean jurídicamente vinculantes, como los dictámenes publicados o el asesoramiento facilitado por ellas. Las acciones contra una autoridad de control deben ejercitarse ante los tribunales del Estado miembro en el que esté establecida y tramitarse con arreglo al Derecho procesal de dicho Estado miembro. Dichos tribunales deben tener plena jurisdicción, incluida la competencia para examinar todos los elementos de hecho y de Derecho relativos a la causa de la que conozcan.

Si una autoridad de control rechaza o desestima una reclamación, el reclamante puede ejercitar una acción ante los tribunales del mismo Estado miembro. En el contexto de las acciones judiciales relacionadas con la aplicación del presente Reglamento, los tribunales nacionales que estimen necesaria una decisión al respecto para poder emitir su fallo pueden, o en el caso establecido en el artículo 267 del TFUE, deben solicitar al Tribunal de Justicia que se pronuncie con carácter prejudicial sobre la interpretación del Derecho de la Unión, incluido el presente Reglamento. Además, si una decisión de una autoridad de control por la que se ejecuta una decisión del Comité se impugna ante un tribunal nacional y se cuestiona la validez de la decisión del Comité, dicho tribunal nacional no es competente para declarar inválida la decisión del Comité, sino que, si la considera inválida, tiene que remitir la cuestión de la validez al Tribunal de Justicia de conformidad con el artículo 267 del TFUE, según la interpretación de este. No obstante, un tribunal nacional puede no remitir la cuestión de la validez de la decisión del Comité a instancia de una persona física o jurídica que, habiendo tenido la oportunidad de interponer recurso de anulación de dicha decisión, en particular si dicha decisión la afectaba directa e individualmente, no lo hizo en el plazo establecido en el artículo 263 del TFUE.

(144) Si un tribunal ante el cual se ejercitaron acciones contra una decisión de una autoridad de control tiene motivos para creer que se ejercitaron acciones ante un tribunal competente de otro Estado miembro relativas al mismo tratamiento, como tener el mismo asunto con respecto a un tratamiento por el mismo responsable o encargado, o la misma causa de la acción, debe ponerse en contacto con ese tribunal para confirmar la existencia de tales acciones conexas. Si dichas acciones conexas están pendientes ante un tribunal de otro Estado miembro,

cualquier otro tribunal distinto de aquel ante el cual se ejercitó la acción en primer lugar puede suspender el procedimiento o, a instancia de una de las partes, inhibirse a favor del tribunal ante el cual se ejercitó la acción en primer lugar si este último es competente para su conocimiento y su acumulación es conforme a Derecho. Se consideran conexas las acciones vinculadas entre sí por una relación tan estrecha que procede tramitarlas y resolverlas conjuntamente a fin de evitar resoluciones que podrían ser incompatibles si se sustanciaran como causas separadas.

(145) Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

(146) El responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento. El responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que en modo alguno son responsables de los daños y perjuicios. El concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos del presente Reglamento. Lo anterior se entiende sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros. Un tratamiento en infracción del presente Reglamento también incluye aquel tratamiento que infringe actos delegados y de ejecución adoptados de conformidad con el presente Reglamento y el Derecho de los Estados miembros que especifique las normas del presente Reglamento. Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos. Si los responsables o encargados participan en el mismo tratamiento, cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios. No obstante, si se acumulan en la misma causa de conformidad con el Derecho de los Estados miembros, la indemnización puede prorratearse en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, siempre que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios. Todo responsable o encargado que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables o encargados que hayan participado en el mismo tratamiento.

(147) En los casos en que el presente Reglamento contiene normas específicas sobre competencia judicial, en particular por lo que respecta a las acciones que tratan de obtener satisfacción por la vía judicial, incluida la indemnización, contra un responsable o encargado del tratamiento, las normas generales de competencia judicial como las establecidas en el Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo ([1]) deben entenderse sin perjuicio de la aplicación de dichas normas específicas.

(148) A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

(149) Los Estados miembros deben tener la posibilidad de establecer normas en materia de sanciones penales por infracciones del presente Reglamento, incluidas las infracciones de normas nacionales adoptadas con arreglo a él y dentro de sus límites. Dichas sanciones penales pueden asimismo autorizar la privación de los beneficios obtenidos en infracción del presente Reglamento. No obstante, la imposición de sanciones penales por infracciones de dichas normas nacionales y de sanciones administrativas no debe entrañar la vulneración del principio *ne bis in idem*, según la interpretación del Tribunal de Justicia.

(150) A fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, cada autoridad de control debe estar facultada para imponer multas administrativas. El presente Reglamento debe

([1]) Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DO L 351 de 20.12.2012, p. 1).

indicar las infracciones así como el límite máximo y los criterios para fijar las correspondientes multas administrativas, que la autoridad de control competente debe determinar en cada caso individual teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo en particular a la naturaleza, gravedad y duración de la infracción y sus consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o mitigar las consecuencias de la infracción. Si las multas administrativas se imponen a una empresa, por tal debe entenderse una empresa con arreglo a los artículos 101 y 102 del TFUE. Si las multas administrativas se imponen a personas que no son una empresa, la autoridad de control debe tener en cuenta al valorar la cuantía apropiada de la multa el nivel general de ingresos prevaleciente en el Estado miembro así como la situación económica de la persona. El mecanismo de coherencia también puede emplearse para fomentar una aplicación coherente de las multas administrativas. Debe corresponder a los Estados miembros determinar si y en qué medida se debe imponer multas administrativas a las autoridades públicas. La imposición de una multa administrativa o de una advertencia no afecta al ejercicio de otras competencias de las autoridades de control ni a la aplicación de otras sanciones al amparo del presente Reglamento.

(151) Los ordenamientos jurídicos de Dinamarca y Estonia no permiten las multas administrativas según lo dispuesto en el presente Reglamento. Las normas sobre multas administrativas pueden ser aplicadas en Dinamarca de tal manera que la multa sea impuesta por los tribunales nacionales competentes en cuanto sanción penal, y en Estonia de tal manera que la multa sea impuesta por la autoridad de control en el marco de un juicio de faltas, siempre que tal aplicación de las normas en dichos Estados miembros tenga un efecto equivalente a las multas administrativas impuestas por las autoridades de control. Por lo tanto los tribunales nacionales competentes deben tener en cuenta la recomendación de la autoridad de control que incoe la multa. En todo caso, las multas impuestas deben ser efectivas, proporcionadas y disuasorias.

(152) En los casos en que el presente Reglamento no armoniza las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en casos de infracciones graves del presente Reglamento, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. La naturaleza de dichas sanciones, ya sea penal o administrativa, debe ser determinada por el Derecho de los Estados miembros.

(153) El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de 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 para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio.

(154) El presente Reglamento permite que, al aplicarlo, se tenga en cuenta el principio de acceso del público a los documentos oficiales. El acceso del público a documentos oficiales puede considerarse de interés público. Los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el Derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo. Ambos Derechos deben conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales y, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el presente Reglamento. La referencia a autoridades y organismos públicos debe incluir, en este contexto, a todas las autoridades u otros organismos a los que se aplica el Derecho de los Estados miembros sobre el acceso del público a documentos. La Directiva 2003/98/CE del Parlamento Europeo y del Consejo ([1]) no altera ni afecta en modo alguno al nivel de protección de las personas

([1]) Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público (DO L 345 de 31.12.2003, p. 90).

físicas con respecto al tratamiento de datos personales con arreglo a las disposiciones del Derecho de la Unión y los Estados miembros y, en particular, no altera las obligaciones ni los derechos establecidos en el presente Reglamento. En concreto, dicha Directiva no debe aplicarse a los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de datos personales, ni a partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización haya quedado establecida por ley como incompatible con el Derecho relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales.

(155) El Derecho de los Estados miembros o los convenios colectivos, incluidos los «convenios de empresa», pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral.

(156) El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y libertades del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos. El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos). Los Estados miembros deben establecer garantías adecuadas para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Debe autorizarse que los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos.

(157) Combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros.

(158) El presente Reglamento también debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no debe se de aplicación a personas fallecidas. Las autoridades públicas o los organismos públicos o privados que llevan registros de interés público deben ser servicios que están obligados, con arreglo al Derecho de la Unión o de los Estados miembros, a adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros de valor perdurable para el interés público general y facilitar acceso a ellos. Los Estados miembros también debe estar autorizados a establecer el tratamiento ulterior de datos personales con fines de archivo, por ejemplo a fin de ofrecer información específica relacionada con el comportamiento político bajo antiguos regímenes de Estados totalitarios, el genocidio, los crímenes contra la humanidad, en particular el Holocausto, o los crímenes de guerra.

(159) El presente Reglamento también debe aplicarse al tratamiento datos personales que se realice con fines de investigación científica. El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas.

(160) El presente Reglamento debe aplicarse asimismo al tratamiento datos personales que se realiza con fines de investigación histórica. Esto incluye asimismo la investigación histórica y la investigación para fines genealógicos, teniendo en cuenta que el presente Reglamento no es de aplicación a personas fallecidas.

(161) Al objeto de otorgar el consentimiento para la participación en actividades de investigación científica en ensayos clínicos, deben aplicarse las disposiciones pertinentes del Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo ([1]).

(162) El presente Reglamento debe aplicarse al tratamiento de datos personales con fines estadísticos. El contenido estadístico, el control de accesos, las especificaciones para el tratamiento de datos personales con fines estadísticos y las medidas adecuadas para salvaguardar los derechos y las libertades de los interesados y garantizar la confidencialidad estadística deben ser establecidos, dentro de los límites del presente Reglamento, por el Derecho de la Unión o de los Estados miembros. Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos. Estos resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica. El fin estadístico implica que el resultado del tratamiento con fines estadísticos no sean datos personales, sino datos agregados, y que este resultado o los datos personales no se utilicen para respaldar medidas o decisiones relativas a personas físicas concretas.

(163) Debe protegerse la información confidencial que las autoridades estadísticas de la Unión y nacionales recojan para la elaboración de las estadísticas oficiales europeas y nacionales. Las estadísticas europeas deben desarrollarse, elaborarse y difundirse con arreglo a los principios estadísticos fijados en el artículo 338, apartado 2, del TFUE, mientras que las estadísticas nacionales deben cumplir asimismo el Derecho de los Estados miembros. El Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo ([2]) facilita especificaciones adicionales sobre la confidencialidad estadística aplicada a las estadísticas europeas.

(164) 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 el deber de secreto profesional u obligaciones equivalentes, en la medida necesaria para conciliar el derecho a la protección de los datos personales con el deber de secreto profesional. Lo anterior se entiende sin perjuicio de las obligaciones existentes para los Estados miembros de adoptar normas sobre el secreto profesional cuando así lo exija el Derecho de la Unión.

(165) El presente Reglamento respeta y no prejuzga el estatuto reconocido en los Estados miembros, en virtud del Derecho constitucional, a las iglesias y las asociaciones o comunidades religiosas, tal como se reconoce en el artículo 17 del TFUE.

(166) 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

([1]) Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE (DO L 158 de 27.5.2014, p. 1).

([2]) Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008 relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) n.º 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas (DO L 87 de 31.3.2009, p. 164).

garantizar la libre circulación de los datos personales en la Unión, debe delegarse en la Comisión el poder de adoptar actos de conformidad con el artículo 290 del TFUE. En particular, deben adoptarse actos delegados en relación con los criterios y requisitos para los mecanismos de certificación, la información que debe presentarse mediante iconos normalizados y los procedimientos para proporcionar dichos iconos. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. 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.

(167) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución cuando así lo establezca el presente Reglamento. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo. En este contexto, la Comisión debe considerar la adopción de medidas específicas para las microempresas y las pequeñas y medianas empresas.

(168) El procedimiento de examen debe seguirse para la adopción de actos de ejecución sobre cláusulas contractuales tipo entre responsables y encargados del tratamiento y entre responsables del tratamiento; códigos de conducta; normas técnicas y mecanismos de certificación; el nivel adecuado de protección ofrecido por un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional; cláusulas tipo de protección; formatos y procedimientos para el intercambio de información entre responsables, encargados y autoridades de control respecto de normas corporativas vinculantes; asistencia mutua; y modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre las autoridades de control y el Comité.

(169) La Comisión debe adoptar actos de ejecución inmediatamente aplicables cuando las pruebas disponibles muestren que un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional no garantizan un nivel de protección adecuado y así lo requieran razones imperiosas de urgencia.

(170) Dado que el objetivo del presente Reglamento, a saber, garantizar un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones o los efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(171) La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Todo tratamiento ya iniciado en la fecha de aplicación del presente Reglamento debe ajustarse al presente Reglamento en el plazo de dos años a partir de la fecha de su entrada en vigor. Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento. Las decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas.

(172) De conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001, se consultó al Supervisor Europeo de Protección de Datos, y éste emitió su dictamen el 7 de marzo de 2012 ([1]).

(173) 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 personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([2]), 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. Una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento.

([1]) DO C 192 de 30.6.2012, p. 7.
([2]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

Disposiciones generales

Artículo 1

Objeto

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;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

3. El Reglamento (CE) n.º 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.

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

Artículo 3

Ámbito 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 en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado 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, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

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

Artículo 4

Definiciones

A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, 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, limitación, supresión o destrucción;

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

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

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

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que

puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

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

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

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

16) «establecimiento principal»:

a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

20) «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 para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c) se ha presentado una reclamación ante esa autoridad de control;

23) «tratamiento transfronterizo»:

a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo ([1]);

26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

CAPÍTULO II

Principios

Artículo 5

Principios relativos al tratamiento

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

([1]) Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 6

Licitud del tratamiento

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

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

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento,

incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Artículo 7

Condiciones para el consentimiento

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

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 previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 8

Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

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

Artículo 9

Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

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 los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

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

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 10

Tratamiento de datos personales relativos a condenas e infracciones penales

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 11

Tratamiento que no requiere identificación

1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

CAPÍTULO III

Derechos del interesado

Sección 1

Transparencia y modalidades

Artículo 12

Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Sección 2

Información y acceso a los datos personales

Artículo 13

Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

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

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) 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 la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14

Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

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

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

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

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;

c) 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 la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

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

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;

b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o

c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

Artículo 15

Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a 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 los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

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

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Sección 3

Rectificación y supresión

Artículo 16

Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 17

Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18

Derecho a la limitación del tratamiento

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

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

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

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19

Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20

Derecho a la portabilidad de los datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Sección 4

Derecho de oposición y decisiones individuales automatizadas

Artículo 21

Derecho de oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22

Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Sección 5

Limitaciones

Artículo 23

Limitaciones

1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

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

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;

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

c) el alcance de las limitaciones establecidas;

d) las garantías para evitar accesos o transferencias ilícitos o abusivos;

e) la determinación del responsable o de categorías de responsables;

f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;

g) los riesgos para los derechos y libertades de los interesados, y

h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

CAPÍTULO IV

Responsable del tratamiento y encargado del tratamiento

Sección 1

Obligaciones generales

Artículo 24

Responsabilidad del responsable del tratamiento

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Artículo 25

Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Artículo 26

Corresponsables del tratamiento

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Artículo 27

Representantes de responsables o encargados del tratamiento no establecidos en la Unión

1. Cuando sea de aplicación el artículo 3, apartado 2, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión.

2. La obligación establecida en el apartado 1 del presente artículo no será aplicable:

a) al tratamiento que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o

b) a las autoridades u organismos públicos.

3. El representante estará establecido en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado.

4. El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en el presente Reglamento.

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

Artículo 28

Encargado del tratamiento

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 29

Tratamiento bajo la autoridad del responsable o del encargado del tratamiento

El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 30

Registro de las actividades de tratamiento

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;

b) las categorías de tratamientos efectuados por cuenta de cada responsable;

c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 31

Cooperación con la autoridad de control

El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

Sección 2

Seguridad de los datos personales

Artículo 32

Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 33

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

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre 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) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34

Comunicación de una violación de la seguridad de los datos personales al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Sección 3

Evaluación de impacto relativa a la protección de datos y consulta previa

Artículo 35

Evaluación de impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable 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.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 36

Consulta previa

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d) en su caso, los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control.

4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

Sección 4

Delegado de protección de datos

Artículo 37

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 lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

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 a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 38

Posición del delegado de protección de datos

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Artículo 39

Funciones del delegado de protección de datos

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Sección 5

Códigos de conducta y certificación

Artículo 40

Códigos de conducta

1. Los Estados miembros, las autoridades de control, el Comité 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 y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:

a) el tratamiento leal y transparente;

b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;

c) la recogida de datos personales;

d) la seudonimización de datos personales;

e) la información proporcionada al público y a los interesados;

f) el ejercicio de los derechos de los interesados;

g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;

h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;

i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;

j) la transferencia de datos personales a terceros países u organizaciones internacionales, o

k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

3. Además de la adhesión de los responsables o encargados del tratamiento a los que se aplica el presente Reglamento, los responsables o encargados a los que no se aplica el presente Reglamento en virtud del artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el apartado 5 del presente artículo y que tengan validez general en virtud del apartado 9 del presente artículo, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra e). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

4. El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apartado 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 51 o 56.

5. Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al artículo 55. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.

6. Si el proyecto de código o la modificación o ampliación es aprobado de conformidad con el apartado 5 y el código de conducta de que se trate no se refiere a actividades de tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código.

7. Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente en virtud del artículo 55 lo presentará por el procedimiento mencionado en el artículo 63, antes de su aprobación o de la modificación o ampliación, al Comité, el cual dictaminará si dicho proyecto, modificación o ampliación es conforme con el presente Reglamento o, en la situación indicada en el apartado 3 del presente artículo, ofrece garantías adecuadas.

8. Si el dictamen a que se refiere el apartado 7 confirma que el proyecto de código o la modificación o ampliación cumple lo dispuesto en el presente Reglamento o, en la situación indicada en el apartado 3, ofrece garantías adecuadas, el Comité presentará su dictamen a la Comisión.

9. La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados con arreglo al apartado 8 del presente artículo tengan validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

10. La Comisión dará publicidad adecuada a los códigos aprobados cuya validez general haya sido decidida de conformidad con el apartado 9.

11. El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 41

Supervisión de códigos de conducta aprobados

1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.

2. El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:

a) ha demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código;

b) ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;

c) ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

d) ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los criterios de acreditación de un organismo a que se refiere el apartado 1 del presente artículo.

4. Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.

5. La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento.

6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.

Artículo 42

Certificación

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

3. La certificación será voluntaria y estará disponible a través de un proceso transparente.

4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56.

5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.

6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.

7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.

8. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 43

Organismo de certificación

1. Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos:

a) la autoridad de control que sea competente en virtud del artículo 55 o 56;

b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo ([1]) con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56.

2. Los organismos de certificación mencionados en el apartado 1 únicamente serán acreditados de conformidad con dicho apartado si:

a) han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación;

([1]) Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

b) se han comprometido a respetar los criterios mencionados en el artículo 42, apartado 5, y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63;

c) han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos;

d) han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

e) han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La acreditación de los organismos de certificación a que se refieren los apartados 1 y 2 del presente artículo se realizará sobre la base de los criterios aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63. En caso de acreditación de conformidad con el apartado 1, letra b), del presente artículo, estos requisitos complementarán los contemplados en el Reglamento (CE) n.º 765/2008 y las normas técnicas que describen los métodos y procedimientos de los organismos de certificación.

4. Los organismos de certificación a que se refiere el apartado 1 serán responsable de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del presente Reglamento. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el presente artículo.

5. Los organismos de certificación a que se refiere el apartado 1 comunicarán a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada.

6. La autoridad de control hará públicos los requisitos a que se refiere el apartado 3 del presente artículo y los criterios a que se a refiere el artículo 42, apartado 5, en una forma fácilmente accesible. Las autoridades de control comunicarán también dichos requisitos y criterios al Comité. El Comité archivará en un registro todos los mecanismos de certificación y sellos de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

7. No obstante lo dispuesto en el capítulo VIII, la autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación a tenor del apartado 1 del presente artículo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el presente Reglamento.

8. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 92, a fin de especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos a que se refiere el artículo 42, apartado 1.

9. La Comisión podrá adoptar actos de ejecución que establezcan normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, y mecanismos para promover y reconocer dichos mecanismos de certificación, sellos y marcas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

CAPÍTULO V

Transferencias de datos personales a terceros países u organizaciones internacionales

Artículo 44

Principio general de las transferencias

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u 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, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 45

Transferencias basadas en una decisión de adecuación

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, 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 u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.

6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el *Diario Oficial de la Unión Europea* y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

Artículo 46

Transferencias mediante garantías adecuadas

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) normas corporativas vinculantes de conformidad con el artículo 47;

c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o 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, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 47

Normas corporativas vinculantes

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos 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) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, 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 de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios 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) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

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

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados 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 a que se refiere el artículo 93, apartado 2.

Artículo 48

Transferencias o comunicaciones no autorizadas por el Derecho de la Unión

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

Artículo 49

Excepciones para situaciones específicas

1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

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

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;

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

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

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

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, 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, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Artículo 50

Cooperación internacional en el ámbito de la protección de datos personales

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 que faciliten la aplicación eficaz 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 adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;

c) asociar a partes interesadas en la materia a 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, inclusive en materia de conflictos de jurisdicción con terceros países.

CAPÍTULO VI

Autoridades de control independientes

Sección 1

Independencia

Artículo 51

Autoridad de control

1. Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII.

3. Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63.

4. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el presente capítulo a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que afecte a dichas disposiciones.

Artículo 52

Independencia

1. Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento.

2. El miembro o los miembros de cada autoridad de control serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.

3. El miembro o los miembros de cada 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 que sea incompatible, remunerada o no.

4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité.

5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada.

6. Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

Artículo 53

Condiciones generales aplicables a los miembros de la autoridad de control

1. Los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente por:

— su Parlamento,

— su Gobierno,

— su Jefe de Estado, o

— un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros.

2. Cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

3. Los miembros darán por concluidas sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria, de conformidad con el Derecho del Estado miembro de que se trate.

4. Un miembro será destituido únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones.

Artículo 54

Normas relativas al establecimiento de la autoridad de control

1. Cada Estado miembro establecerá por ley todos los elementos indicados a continuación:

a) el establecimiento de cada autoridad de control;

b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control;

c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;

d) la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado;

e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;

f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.

2. El miembro o miembros y el personal de cada autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento.

Sección 2

Competencia, funciones y poderes

Artículo 55

Competencia

1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro.

2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el artículo 56.

3. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

Artículo 56

Competencia de la autoridad de control principal

1. Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

2. No obstante lo dispuesto en el apartado 1, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro.

3. En los casos a que se refiere el apartado 2 del presente artículo, la autoridad de control informará sin dilación al respecto a la autoridad de control principal. En el plazo de tres semanas después de haber sido informada, la autoridad de control principal decidirá si tratará o no el caso de conformidad con el procedimiento establecido en el artículo 60, teniendo presente si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado.

4. En caso de que la autoridad de control principal decida tratar el caso, se aplicará el procedimiento establecido en el artículo 60. La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión. La autoridad de control principal tendrá en cuenta en la mayor medida posible dicho proyecto al preparar el proyecto de decisión a que se refiere el artículo 60, apartado 3.

5. En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará con arreglo a los artículos 61 y 62.

6. La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado.

Artículo 57

Funciones

1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

a) controlar la aplicación del presente Reglamento y hacerlo aplicar;

b) promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención;

c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;

d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento;

e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;

f) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

g) cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento;

h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;

i) hacer un seguimiento de cambios que sean 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 las prácticas comerciales;

j) adoptar las cláusulas contractuales tipo a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

k) elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4;

l) ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2;

m) alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5;

n) fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5;

o) llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas en virtud del artículo 42, apartado 7;

p) elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

q) efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

r) autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3;

s) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47;

t) contribuir a las actividades del Comité;

u) llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2, y

v) desempeñar cualquier otra función relacionada con la protección de los datos personales.

2. Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

3. El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Artículo 58

Poderes

1. Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación:

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

b) llevar a cabo investigaciones en forma de auditorías de protección de datos;

c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

a) sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;

h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

3. Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;

b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;

d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5;

e) acreditar los organismos de certificación con arreglo al artículo 43;

f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;

g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);

i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);

j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.

4. El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.

5. Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.

6. Cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del capítulo VII.

Artículo 59

Informe de actividad

Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité.

CAPÍTULO VII

Cooperación y coherencia

Sección 1

Cooperación y coherencia

Artículo 60

Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas

1. La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente.

2. La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.

3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.

4. En caso de que cualquiera de las autoridades de control interesadas formule una objeción pertinente y motivada acerca del proyecto de decisión en un plazo de cuatro semanas a partir de la consulta con arreglo al apartado 3 del presente artículo, la autoridad de control principal someterá el asunto, en caso de que no siga lo indicado en la objeción pertinente y motivada o estime que dicha objeción no es pertinente o no está motivada, al mecanismo de coherencia contemplado en el artículo 63.

5. En caso de que la autoridad de control principal prevea seguir lo indicado en la objeción pertinente y motivada recibida, presentará a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado. Dicho proyecto de decisión revisado se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas.

6. En caso de que ninguna otra autoridad de control interesada haya presentado objeciones al proyecto de decisión transmitido por la autoridad de control principal en el plazo indicado en los apartados 4 y 5, se considerará que la autoridad de control principal y las autoridades de control interesadas están de acuerdo con dicho proyecto de decisión y estarán vinculadas por este.

7. La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante.

8. No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento.

9. En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado.

10. Tras recibir la notificación de la decisión de la autoridad de control principal con arreglo a los apartados 7 y 9, el responsable o el encargado del tratamiento adoptará las medidas necesarias para garantizar el cumplimiento de la decisión en lo tocante a las actividades de tratamiento en el contexto de todos sus establecimientos en la Unión. El responsable o el encargado notificarán las medidas adoptadas para dar cumplimiento a dicha decisión a la autoridad de control principal, que a su vez informará a las autoridades de control interesadas.

11. En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66.

12. La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado.

Artículo 61

Asistencia mutua

1. Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua a fin de aplicar el presente Reglamento de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones.

2. Cada autoridad de control adoptará todas las medidas oportunas requeridas para responder a una solicitud de otra autoridad de control sin dilación indebida y a más tardar en el plazo de un mes a partir de la solicitud. Dichas medidas podrán incluir, en particular, la transmisión de información pertinente sobre el desarrollo de una investigación.

3. Las solicitudes de asistencia deberán contener toda la información necesaria, entre otras cosas respecto de la finalidad y los motivos de la solicitud. La información que se intercambie se utilizará únicamente para el fin para el que haya sido solicitada.

4. La autoridad de control requerida no podrá negarse a responder a una solicitud, salvo si:

a) no es competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita, o

b) el hecho de responder a la solicitud infringiría el presente Reglamento o el Derecho de la Unión o de los Estados miembros que se aplique a la autoridad de control a la que se dirigió la solicitud.

5. La autoridad de control requerida informará a la autoridad de control requirente de los resultados obtenidos o, en su caso, de los progresos registrados o de las medidas adoptadas para responder a su solicitud. La autoridad de control requerida explicará los motivos de su negativa a responder a una solicitud al amparo del apartado 4.

6. Como norma general, las autoridades de control requeridas facilitarán la información solicitada por otras autoridades de control por medios electrónicos, utilizando un formato normalizado.

7. Las autoridades de control requeridas no cobrarán tasa alguna por las medidas adoptadas a raíz de una solicitud de asistencia mutua. Las autoridades de control podrán convenir normas de indemnización recíproca por gastos específicos derivados de la prestación de asistencia mutua en circunstancias excepcionales.

8. Cuando una autoridad de control no facilite la información mencionada en el apartado 5 del presente artículo en el plazo de un mes a partir de la recepción de la solicitud de otra autoridad de control, la autoridad de control requirente podrá adoptar una medida provisional en el territorio de su Estado miembro de conformidad con lo dispuesto en el artículo 55, apartado 1. En ese caso, se supondrá que existe la necesidad urgente contemplada en el artículo 66, apartado 1, que exige una decisión urgente y vinculante del Comité en virtud del artículo 66, apartado 2.

9. La Comisión podrá, mediante actos de ejecución, especificar el formato y los procedimientos de asistencia mutua contemplados en el presente artículo, así como las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité, en especial el formato normalizado mencionado en el apartado 6 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 62

Operaciones conjuntas de las autoridades de control

1. Las autoridades de control realizarán, en su caso, operaciones conjuntas, incluidas investigaciones conjuntas y medidas de ejecución conjuntas, en las que participen miembros o personal de las autoridades de control de otros Estados miembros.

2. Si el responsable o el encargado del tratamiento tiene establecimientos en varios Estados miembros o si es probable que un número significativo de interesados en más de un Estado miembro se vean sustancialmente afectados por las operaciones de tratamiento, una autoridad de control de cada uno de esos Estados miembros tendrá derecho a participar en operaciones conjuntas. La autoridad de control que sea competente en virtud del artículo 56, apartados 1 o 4, invitará a la autoridad de control de cada uno de dichos Estados miembros a participar en las operaciones conjuntas y responderá sin dilación a la solicitud de participación presentada por una autoridad de control.

3. Una autoridad de control podrá, con arreglo al Derecho de su Estado miembro y con la autorización de la autoridad de control de origen, conferir poderes, incluidos poderes 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 el Derecho del Estado miembro de la autoridad de control de acogida, que los miembros o el personal de la autoridad de control de origen ejerzan sus poderes de investigación de conformidad con el Derecho del Estado miembro de la autoridad de control de origen. Dichos poderes de investigación solo podrán ejercerse bajo la orientación y 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 del Estado miembro de la autoridad de control de acogida.

4. Cuando participe, de conformidad con el apartado 1, personal de la autoridad de control de origen en operaciones en otro Estado miembro, el Estado miembro de la autoridad de control de acogida asumirá la responsabilidad de acuerdo con el Derecho del Estado miembro en cuyo territorio se desarrollen las operaciones, por los daños y perjuicios que haya causado dicho personal en el transcurso de las mismas.

5. El Estado miembro en cuyo territorio se causaron los daños y perjuicios asumirá su reparación en las condiciones aplicables a los daños y perjuicios causados por su propio personal. El Estado miembro de la autoridad de control de origen cuyo personal haya causado daños y perjuicios a cualquier persona en el territorio de otro Estado miembro le restituirá íntegramente los importes que este último haya abonado a los derechohabientes.

6. Sin perjuicio del ejercicio de sus derechos frente a terceros y habida cuenta de la excepción establecida en el apartado 5, los Estados miembros renunciarán, en el caso contemplado en el apartado 1, a solicitar de otro Estado miembro el reembolso del importe de los daños y perjuicios mencionados en el apartado 4.

7. Cuando se prevea una operación conjunta y una autoridad de control no cumpla en el plazo de un mes con la obligación establecida en el apartado 2, segunda frase, del presente artículo, las demás autoridades de control podrán adoptar una medida provisional en el territorio de su Estado miembro de conformidad con el artículo 55. En ese caso, se presumirá la existencia de una necesidad urgente a tenor del artículo 66, apartado 1, y se requerirá dictamen o decisión vinculante urgente del Comité en virtud del artículo 66, apartado 2.

Sección 2

Coherencia

Artículo 63

Mecanismo de coherencia

A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección.

Artículo 64

Dictamen del Comité

1. El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión:

a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;

b) afecte a un asunto de conformidad con el artículo 40, apartado 7, cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento;

c) tenga por objeto aprobar los criterios aplicables a la acreditación de un organismo con arreglo al artículo 41, apartado 3, o un organismo de certificación conforme al artículo 43, apartado 3;

d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, letra d), y el artículo 28, apartado 8;

e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, letra a);

f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del artículo 47.

2. Cualquier autoridad de control, el presidente del Comité o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61 o las operaciones conjuntas con arreglo al artículo 62.

3. En los casos a que se refieren los apartados 1 y 2, el Comité emitirá dictamen sobre el asunto que le haya sido presentado siempre que no haya emitido ya un dictamen sobre el mismo asunto. Dicho dictamen se adoptará en el plazo de ocho semanas por mayoría simple de los miembros del Comité. Dicho plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Por lo que respecta al proyecto de decisión a que se refiere el apartado 1 y distribuido a los miembros del Comité con arreglo al apartado 5, todo miembro que no haya presentado objeciones dentro de un plazo razonable indicado por el presidente se considerará conforme con el proyecto de decisión.

4. Las autoridades de control y la Comisión comunicarán sin dilación por vía electrónica al Comité, utilizando un formato normalizado, toda información útil, en particular, cuando proceda, un resumen de los hechos, el proyecto de decisión, los motivos por los que es necesaria tal medida, y las opiniones de otras autoridades de control interesadas.

5. La Presidencia del Comité informará sin dilación indebida por medios electrónicos:

a) a los miembros del Comité y a la Comisión de cualquier información pertinente que le haya sido comunicada, utilizando un formato normalizado. La secretaría del Comité facilitará, de ser necesario, traducciones de la información que sea pertinente, y

b) a la autoridad de control contemplada, en su caso, en los apartados 1 y 2 y a la Comisión del dictamen, y lo publicará.

6. La autoridad de control competente no adoptará su proyecto de decisión a tenor del apartado 1 en el plazo mencionado en el apartado 3.

7. La autoridad de control contemplada en el artículo 1 tendrá en cuenta en la mayor medida posible el dictamen del Comité y, en el plazo de dos semanas desde la recepción del dictamen, comunicará por medios electrónicos al presidente del Comité si va a mantener o modificar su proyecto de decisión y, si lo hubiera, el proyecto de decisión modificado, utilizando un formato normalizado.

8. Cuando la autoridad de control interesada informe al presidente del Comité, en el plazo mencionado en el apartado 7 del presente artículo, de que no prevé seguir el dictamen del Comité, en todo o en parte, alegando los motivos correspondientes, se aplicará el artículo 65, apartado 1.

Artículo 65

Resolución de conflictos por el Comité

1. Con el fin de garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante en los siguientes casos:

a) cuando, en un caso mencionado en el artículo 60, apartado 4, una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad principal, o esta haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos a que se refiera la objeción pertinente y motivada, en particular si hay infracción del presente Reglamento;

b) cuando haya puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal;

c) cuando una autoridad de control competente no solicite dictamen al Comité en los casos contemplados en el artículo 64, apartado 1, o no siga el dictamen del Comité emitido en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, lo pondrá en conocimiento del Comité.

2. La decisión a que se refiere el apartado 1 se adoptará en el plazo de un mes a partir de la remisión del asunto, por mayoría de dos tercios de los miembros del Comité. Este plazo podrá prorrogarse un mes más, habida cuenta de la complejidad del asunto. La decisión que menciona el apartado 1 estará motivada y será dirigida a la autoridad de control principal y a todas las autoridades de control interesadas, y será vinculante para ellas.

3. Cuando el Comité no haya podido adoptar una decisión en los plazos mencionados en el apartado 2, adoptará su decisión en un plazo de dos semanas tras la expiración del segundo mes a que se refiere el apartado 2, por mayoría simple de sus miembros. En caso de empate, decidirá el voto del presidente.

4. Las autoridades de control interesadas no adoptarán decisión alguna sobre el asunto presentado al Comité en virtud del apartado 1 durante los plazos de tiempo a que se refieren los apartados 2 y 3.

5. El presidente del Comité notificará sin dilación indebida la decisión contemplada en el apartado 1 a las autoridades de control interesadas. También informará de ello a la Comisión. La decisión se publicará en el sitio web del Comité sin demora, una vez que la autoridad de control haya notificado la decisión definitiva a que se refiere el apartado 6.

6. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de la decisión contemplada en el apartado 1 del presente artículo, sin dilación indebida y a más tardar un mes tras la notificación de la decisión del Comité. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación informará al Comité de la fecha de notificación de su decisión definitiva al responsable o al encargado del tratamiento y al interesado, respectivamente. La decisión definitiva de las autoridades de control interesadas será adoptada en los términos establecidos en el artículo 60, apartados 7, 8 y 9. La decisión definitiva hará referencia a la decisión contemplada en el apartado 1 del presente artículo y especificará que esta última decisión se publicará en el sitio web del Comité con arreglo al apartado 5 del presente artículo. La decisión definitiva llevará adjunta la decisión contemplada en el apartado 1 del presente artículo.

Artículo 66

Procedimiento de urgencia

1. En circunstancias excepcionales, cuando una autoridad de control interesada considere que es urgente intervenir para proteger los derechos y las libertades de interesados, podrá, como excepción al mecanismo de coherencia contemplado en los artículos 63, 64 y 65, o al procedimiento mencionado en el artículo 60, adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un periodo de validez determinado que no podrá ser superior a tres meses. La autoridad de control comunicará sin dilación dichas medidas, junto con los motivos de su adopción, a las demás autoridades de control interesadas, al Comité y a la Comisión.

2. Cuando una autoridad de control haya adoptado una medida de conformidad con el apartado 1, y considere que deben adoptarse urgentemente medidas definitivas, podrá solicitar con carácter urgente un dictamen o una decisión vinculante urgente del Comité, motivando dicha solicitud de dictamen o decisión.

3. Cualquier autoridad de control podrá solicitar, motivando su solicitud, y, en particular, la urgencia de la intervención, un dictamen urgente o una decisión vinculante urgente, según el caso, del Comité, cuando una autoridad de control competente no haya tomado una medida apropiada en una situación en la que sea urgente intervenir a fin de proteger los derechos y las libertades de los interesados.

4. No obstante lo dispuesto en el artículo 64, apartado 3, y en el artículo 65, apartado 2, los dictámenes urgentes o decisiones vinculantes 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 Comité.

Artículo 67

Intercambio de información

La Comisión podrá adoptar actos de ejecución de ámbito general para especificar las modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre dichas autoridades y el Comité, en especial el formato normalizado contemplado en el artículo 64.

Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Sección 3

Comité europeo de protección de datos

Artículo 68

Comité Europeo de Protección de Datos

1. Se crea el Comité Europeo de Protección de Datos («Comité»), como organismo de la Unión, que gozará de personalidad jurídica.

2. El Comité estará representado por su presidente.

3. El Comité estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos.

4. Cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro.

5. La Comisión tendrá derecho a participar en las actividades y reuniones del Comité, sin derecho a voto. La Comisión designará un representante. El presidente del Comité comunicará a la Comisión las actividades del Comité.

6. En los casos a que se refiere el artículo 65, el Supervisor Europeo de Protección de Datos sólo tendrá derecho a voto en las decisiones relativas a los principios y normas aplicables a las instituciones, órganos y organismos de la Unión que correspondan en cuanto al fondo a las contempladas en el presente Reglamento.

Artículo 69

Independencia

1. El Comité actuará con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias con arreglo a los artículos 70 y 71.

2. Sin perjuicio de las solicitudes de la Comisión contempladas en el artículo 70, apartado 1, letra b), y apartado 2, el Comité no solicitará ni admitirá instrucciones de nadie en el desempeño de sus funciones o el ejercicio de sus competencias.

Artículo 70

Funciones del Comité

1. El Comité garantizará la aplicación coherente del presente Reglamento. A tal efecto, el Comité, a iniciativa propia o, en su caso, a instancia de la Comisión, en particular:

a) supervisará y garantizará la correcta aplicación del presente Reglamento en los casos contemplados en los artículos 64 y 65, sin perjuicio de las funciones de las autoridades de control nacionales;

b) 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;

c) asesorará a la Comisión sobre el formato y los procedimientos para intercambiar información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes;

d) emitirá directrices, recomendaciones y buenas prácticas relativas a los procedimientos para la supresión de vínculos, copias o réplicas de los datos personales procedentes de servicios de comunicación a disposición pública a que se refiere el artículo 17, apartado 2;

e) examinará, a iniciativa propia, 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 buenas prácticas a fin de promover la aplicación coherente del presente Reglamento;

f) emitirá directrices, recomendaciones y buenas prácticas de conformidad con la letra e) del presente apartado a fin de especificar más los criterios y requisitos de las decisiones basadas en perfiles en virtud del artículo 22, apartado 2;

g) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de constatar las violaciones de la seguridad de los datos y determinar la dilación indebida a tenor del artículo 33, apartados 1 y 2, y con respecto a las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales;

h) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con respecto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas a tenor del artículo 34, apartado 1;

i) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con el fin de especificar en mayor medida los criterios y requisitos para las transferencias de datos personales basadas en normas corporativas vinculantes a las que se hayan adherido los responsables del tratamiento y en normas corporativas vinculantes a las que se hayan adherido los encargados del tratamiento y en requisitos adicionales necesarios para garantizar la protección de los datos personales de los interesados a que se refiere el artículo 47;

j) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de especificar en mayor medida los criterios y requisitos de las transferencias de datos personales sobre la base del artículo 49, apartado 1;

k) formulará directrices para las autoridades de control, relativas a la aplicación de las medidas a que se refiere el artículo 58, apartados 1, 2 y 3, y la fijación de multas administrativas de conformidad con el artículo 83;

l) examinará la aplicación práctica de las directrices, recomendaciones y buenas prácticas a que se refieren las letras e) y f);

m) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de establecer procedimientos comunes de información procedente de personas físicas sobre infracciones del presente Reglamento en virtud del artículo 54, apartado 2;

n) alentará la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos de conformidad con los artículos 40 y 42;

o) realizará la acreditación de los organismos de certificación y su revisión periódica en virtud del artículo 43, y llevará un registro público de los organismos acreditados en virtud del artículo 43, apartado 6, y de los responsables o los encargados del tratamiento acreditados establecidos en terceros países en virtud del artículo 42, apartado 7;

p) especificará los requisitos contemplados en el artículo 43, apartado 3, con miras a la acreditación de los organismos de certificación en virtud del artículo 42;

q) facilitará a la Comisión un dictamen sobre los requisitos de certificación contemplados en el artículo 43, apartado 8;

r) facilitará a la Comisión un dictamen sobre los iconos a que se refiere el artículo 12, apartado 7;

s) facilitará a la Comisión un dictamen para evaluar la adecuación del nivel de protección en un tercer país u organización internacional, en particular para evaluar si un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o una organización internacional, ya no garantizan un nivel de protección adecuado. A tal fin, la Comisión facilitará al Comité toda la documentación necesaria, incluida la correspondencia con el gobierno del tercer país, que se refiera a dicho tercer país, territorio o específico o a dicha organización internacional;

t) emitirá dictámenes sobre los proyectos de decisión de las autoridades de control en virtud del mecanismo de coherencia mencionado en el artículo 64, apartado 1, sobre los asuntos presentados en virtud del artículo 64, apartado 2, y sobre las decisiones vinculantes en virtud del artículo 65, incluidos los casos mencionados en el artículo 66;

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

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

w) promoverá el intercambio de conocimientos y documentación sobre legislación y prácticas en materia de protección de datos con las autoridades de control encargadas de la protección de datos a escala mundial;

x) emitirá dictámenes sobre los códigos de conducta elaborados a escala de la Unión de conformidad con el artículo 40, apartado 9, y

y) llevará un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

2. Cuando la Comisión solicite asesoramiento del Comité podrá señalar un plazo teniendo en cuenta la urgencia del asunto.

3. El Comité transmitirá sus dictámenes, directrices, recomendaciones y buenas prácticas a la Comisión y al Comité contemplado en el artículo 93, y los hará públicos.

4. Cuando proceda, el Comité consultará a las partes interesadas y les dará la oportunidad de presentar sus comentarios en un plazo razonable. Sin perjuicio de lo dispuesto en el artículo 76, el Comité publicará los resultados del procedimiento de consulta.

Artículo 71

Informes

1. El Comité elaborará un informe anual en materia de protección de las personas físicas en lo que respecta al tratamiento en la Unión y, si procede, en terceros países y organizaciones internacionales. El informe se hará público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión.

2. El informe anual incluirá un examen de la aplicación práctica de las directrices, recomendaciones y buenas prácticas indicadas en el artículo 70, apartado 1, letra l), así como de las decisiones vinculantes indicadas en el artículo 65.

Artículo 72

Procedimiento

1. El Comité tomará sus decisiones por mayoría simple de sus miembros, salvo que el presente Reglamento disponga otra cosa.

2. El Comité adoptará su reglamento interno por mayoría de dos tercios de sus miembros y organizará sus disposiciones de funcionamiento.

Artículo 73

Presidencia

1. El Comité elegirá por mayoría simple de entre sus miembros un presidente y dos vicepresidentes.

2. El mandato del presidente y de los vicepresidentes será de cinco años de duración y podrá renovarse una vez.

Artículo 74

Funciones del presidente

1. El presidente desempeñará las siguientes funciones:

a) convocar las reuniones del Comité y preparar su orden del día;

b) notificar las decisiones adoptadas por el Comité con arreglo al artículo 65 a la autoridad de control principal y a las autoridades de control interesadas;

c) garantizar el ejercicio puntual de las funciones del Comité, en particular en relación con el mecanismo de coherencia a que se refiere el artículo 63.

2. El Comité determinará la distribución de funciones entre el presidente y los vicepresidentes en su reglamento interno.

Artículo 75

Secretaría

1. El Comité contará con una secretaría, de la que se hará cargo el Supervisor Europeo de Protección de Datos.

2. La secretaría ejercerá sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité.

3. El personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento dependerá de un superior jerárquico distinto del personal que desempeñe las funciones conferidas al Supervisor Europeo de Protección de Datos.

4. El Comité, en consulta con el Supervisor Europeo de Protección de Datos, elaborará y publicará, si procede, un memorando de entendimiento para la puesta en práctica del presente artículo, que determinará los términos de su cooperación y que será aplicable al personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento.

5. La secretaría prestará apoyo analítico, administrativo y logístico al Comité.

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

a) los asuntos corrientes del Comité;

b) la comunicación entre los miembros del Comité, su presidente y la Comisión;

c) la comunicación con otras instituciones y con el público;

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

e) la traducción de la información pertinente;

f) la preparación y el seguimiento de las reuniones del Comité;

g) la preparación, redacción y publicación de dictámenes, decisiones relativas a solución de diferencias entre autoridades de control y otros textos adoptados por el Comité.

Artículo 76

Confidencialidad

1. Los debates del Comité serán confidenciales cuando el mismo lo considere necesario, tal como establezca su reglamento interno.

2. El acceso a los documentos presentados a los miembros del Comité, los expertos y los representantes de terceras partes se regirá por el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo ([1]).

CAPÍTULO VIII

Recursos, responsabilidad y sanciones

Artículo 77

Derecho a presentar una reclamación ante una autoridad de control

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.

2. La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 78.

Artículo 78

Derecho a la tutela judicial efectiva contra una autoridad de control

1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente en virtud de los artículos 55 y 56 no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77.

3. Las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control.

4. Cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o una decisión del Comité en el marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión.

Artículo 79

Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento

1. Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

2. Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

([1]) Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

Artículo 80

Representación de los interesados

1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.

2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento.

Artículo 81

Suspensión de los procedimientos

1. Cuando un tribunal competente de un Estado miembro tenga información de la pendencia ante un tribunal de otro Estado miembro de un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado, se pondrá en contacto con dicho tribunal de otro Estado miembro para confirmar la existencia de dicho procedimiento.

2. Cuando un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado esté pendiente ante un tribunal de otro Estado miembro, cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento.

3. Cuando dicho procedimiento esté pendiente en primera instancia, cualquier tribunal distinto de aquel ante el que se ejercitó la acción en primer lugar podrá también, a instancia de una de las partes, inhibirse en caso de que el primer tribunal sea competente para su conocimiento y su acumulación sea conforme a Derecho.

Artículo 82

Derecho a indemnización y responsabilidad

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2.

6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2.

Artículo 83

Condiciones generales para la imposición de multas administrativas

1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 84

Sanciones

1. Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable.

CAPÍTULO IX

Disposiciones relativas a situaciones específicas de tratamiento

Artículo 85

Tratamiento y libertad de expresión y de información

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.

3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

Artículo 86

Tratamiento y acceso del público a documentos oficiales

Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento.

Artículo 87

Tratamiento del número nacional de identificación

Los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento.

Artículo 88

Tratamiento en el ámbito laboral

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 89

Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para

garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

3. Cuando se traten datos personales con fines de archivo en interés público, el Derecho de le Unión o de los Estados miembros podrá prever excepciones a los derechos contemplados en los artículos 15, 16, 18, 19, 20 y 21, sujetas a las condiciones y garantías citadas en el apartado 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

4. En caso de que el tratamiento a que hacen referencia los apartados 2 y 3 sirva también al mismo tiempo a otro fin, las excepciones solo serán aplicables al tratamiento para los fines mencionados en dichos apartados.

Artículo 90

Obligaciones de secreto

1. Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control establecidos en el artículo 58, apartado 1, letras e) y f), en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes, cuando sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto. Esas normas solo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado o con ocasión de una actividad cubierta por la citada obligación de secreto.

2. Cada Estado miembro notificará a la Comisión las normas adoptadas de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 91

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, tales normas podrán seguir aplicándose, siempre que sean conformes con el presente Reglamento.

2. Las iglesias y las asociaciones religiosas que apliquen normas generales de conformidad con el apartado 1 del presente artículo estarán sujetas al control de una autoridad de control independiente, que podrá ser específica, siempre que cumpla las condiciones establecidas en el capítulo VI del presente Reglamento.

CAPÍTULO X

Actos delegados y actos de ejecución

Artículo 92

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 indicada en el artículo 12, apartado 8, y en el artículo 43, apartado 8, se otorgarán a la Comisión por tiempo indefinido a partir del 24 de mayo de 2016.

3. La delegación de poderes mencionada en el artículo 12, apartado 8, y el artículo 43, apartado 8, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto al día siguiente de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en la misma. 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. Los actos delegados adoptados en virtud del artículo 12, apartado 8, y el artículo 43, apartado 8, entrarán en vigor únicamente si, en un plazo de tres meses desde su notificación al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. El plazo se ampliará en tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 93

Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. Cuando se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

3. Cuando se haga referencia al presente apartado, se aplicará el artículo 8 del Reglamento (UE) n.º 182/2011, en relación con su artículo 5.

CAPÍTULO XI

Disposiciones finales

Artículo 94

Derogación de la Directiva 95/46/CE

1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018.

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 establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.

Artículo 95

Relación con la Directiva 2002/58/CE

El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE.

Artículo 96

Relación con acuerdos celebrados anteriormente

Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados por los Estados miembros antes del 24 de mayo de 2016 y que cumplan lo dispuesto en el Derecho de la Unión aplicable antes de dicha fecha, seguirán en vigor hasta que sean modificados, sustituidos o revocados.

Artículo 97

Informes de la Comisión

1. A más tardar el 25 de mayo de 2020 y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.

2. En el marco de las evaluaciones y revisiones a que se refiere el apartado 1, la Comisión examinará en particular la aplicación y el funcionamiento de:

a) el capítulo V sobre la transferencia de datos personales a países terceros u organizaciones internacionales, particularmente respecto de las decisiones adoptadas en virtud del artículo 45, apartado 3, del presente Reglamento, y de las adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE;

b) el capítulo VII sobre cooperación y coherencia.

3. A los efectos del apartado 1, la Comisión podrá solicitar información a los Estados miembros y a las autoridades de control.

4. Al llevar a cabo las evaluaciones y revisiones indicadas en los apartados 1 y 2, la Comisión tendrá en cuenta las posiciones y conclusiones del Parlamento Europeo, el Consejo y los demás órganos o fuentes pertinentes.

5. La Comisión presentará, en caso necesario, las propuestas oportunas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de las tecnologías de la información y a la vista de los progresos en la sociedad de la información.

Artículo 98

Revisión de otros actos jurídicos de la Unión en materia de protección de datos

La Comisión presentará, si procede, propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos.

Artículo 99

Entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. Será aplicable a partir del 25 de mayo de 2018.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 27 de abril de 2016.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*La Presidenta*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

DIRECTIVAS

DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 27 de abril de 2016

relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

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

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Comité de las Regiones ([1]),

De conformidad con el procedimiento legislativo ordinario ([2]),

Considerando lo siguiente:

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

(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos personales. La presente Directiva pretende contribuir a la consecución de un espacio de libertad, seguridad y justicia.

(3) La rápida evolución tecnológica y la globalización han planteado nuevos retos en el ámbito de la protección de los datos personales. Se ha incrementado de manera significativa la magnitud de la recogida y del intercambio de datos personales. La tecnología permite el tratamiento de los datos personales en una escala sin precedentes para la realización de actividades como la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.

(4) Debe ser facilitada la libre circulación de datos personales entre las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública en el seno de la Unión y la transferencia de estos datos personales a terceros países y organizaciones internacionales, al tiempo que se garantiza un alto nivel de protección de los datos personales. Estos avances exigen el establecimiento de un marco más sólido y coherente para la protección de datos personales en la Unión Europea, que cuente con el respaldo de una ejecución estricta.

(5) La Directiva 95/46/CE del Parlamento Europeo y del Consejo ([3]) es de aplicación a todas las actividades relacionadas con el tratamiento de datos personales que tengan lugar en los Estados miembros, tanto en el sector público como en el privado. No se aplica, sin embargo, al tratamiento de datos personales que se efectúe «en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario», como es el caso de las actividades en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.

([1]) DO C 391 de 18.12.2012, p. 127.
([2]) Posición del Parlamento Europeo de 12 de marzo de 2014 (pendiente de publicación en el Diario Oficial) y posición del Consejo en primera lectura de 8 de abril de 2016 (pendiente de publicación en el Diario Oficial). Posición del Parlamento Europeo de 14 de abril de 2016.
([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).

(6) La Decisión Marco 2008/977/JAI del Consejo ([1]) es de aplicación en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial. El ámbito de aplicación de dicha Decisión Marco se limita al tratamiento de los datos personales transmitidos o puestos a disposición entre los Estados miembros.

(7) Para garantizar la eficacia de la cooperación judicial en materia penal y de la cooperación policial, es esencial asegurar un nivel uniforme y elevado de protección de los datos personales de las personas físicas y facilitar el intercambio de datos personales entre las autoridades competentes de los Estados miembros. A tal efecto, el nivel de protección de los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública, debe ser equivalente en todos los Estados miembros. La protección eficaz de los datos personales en toda la Unión requiere tanto el fortalecimiento de los derechos de los interesados y de las obligaciones de quienes tratan dichos datos personales, como el fortalecimiento de los poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos personales en los Estados miembros.

(8) El artículo 16, apartado 2, del TFUE exige que el Parlamento Europeo y el Consejo establezcan las normas sobre la protección de las personas físicas respecto del tratamiento de los datos de carácter personal y sobre la libre circulación de estos datos.

(9) Sobre esa base, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([2]) establece las normas generales para la protección de las personas físicas en relación con el tratamiento de los datos personales y para garantizar la libre circulación de datos personales dentro de la Unión.

(10) En la Declaración n.º 21 relativa a la protección de datos de carácter personal en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial, aneja al acta final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa, la Conferencia reconoció que podrían requerirse normas específicas sobre protección de datos personales y libre circulación de los mismos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial basada en el artículo 16 del TFUE, en razón de la naturaleza específica de dichos ámbitos.

(11) Conviene por lo tanto que esos ámbitos estén regulados por una directiva que establezca las normas específicas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública. Entre dichas autoridades competentes no solo se deben incluir autoridades públicas tales como las autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad, sino también cualquier otro organismo o entidad en que el Derecho del Estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas a los efectos de la presente Directiva. Cuando dicho organismo o entidad trate datos personales con fines distintos de los previstos en la presente Directiva, se aplica el Reglamento (UE) 2016/679. Así pues, el Reglamento (UE) 2016/679 se aplica en los casos en los que un organismo o entidad recopile datos personales con otros fines y proceda a su tratamiento para el cumplimiento de una obligación jurídica a la que esté sujeto. Por ejemplo, con fines de investigación, detección o enjuiciamiento de infracciones penales, las instituciones financieras conservan determinados datos personales que ellas mismas tratan y únicamente facilitan dichos datos personales a las autoridades nacionales competentes en casos concretos y de conformidad con el Derecho del Estado miembro. Todo organismo o entidad que trate datos personales en nombre de las citadas autoridades dentro del ámbito de aplicación de la presente Directiva debe quedar obligado por un contrato u otro acto jurídico y por las disposiciones aplicables a los encargados del tratamiento con arreglo a la presente Directiva, mientras que la aplicación del Reglamento (UE) 2016/679 permanece inalterada para el tratamiento de datos personales por encargados del tratamiento fuera del ámbito de aplicación de la presente Directiva.

(12) Las actividades realizadas por la policía u otras fuerzas y cuerpos de seguridad se centran principalmente en la prevención, investigación, detección o enjuiciamiento de infracciones penales, incluidas las actuaciones policiales en las que no hay constancia de si un incidente es o no constitutivo de infracción penal. También pueden incluir el ejercicio de la autoridad mediante medidas coercitivas, como es el caso de las actuaciones policiales en manifestaciones, grandes acontecimientos deportivos y disturbios. Entre dichas actividades también figura el

([1]) 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).

([2]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (véase la página 1 del presente Diario Oficial).

mantenimiento del orden público, como labor encomendada a la policía o, en su caso, a otras fuerzas y cuerpos de seguridad con fines de protección y prevención frente a las amenazas para la seguridad pública y para los intereses públicos fundamentales jurídicamente protegidos que puedan ser constitutivas de infracciones penales. Los Estados miembros pueden encomendar a las autoridades competentes otras funciones que no necesariamente se lleven a cabo con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública, en cuyo caso el tratamiento de datos personales con estos otros fines, en la medida en que esté comprendido en el ámbito de aplicación del Derecho de la Unión, entrará dentro del ámbito de aplicación del Reglamento (UE) 2016/679.

(13) Una infracción penal en el sentido de lo dispuesto en la presente Directiva debe ser un concepto autónomo del Derecho de la Unión, tal y como lo interpreta el Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia»).

(14) Puesto que la presente Directiva no debe aplicarse al tratamiento de datos personales en el marco de una actividad que no esté comprendida en el ámbito de aplicación del Derecho de la Unión, no deben considerarse comprendidas en el ámbito de aplicación de la presente Directiva las actividades relacionadas con la seguridad nacional, las actividades de los servicios o unidades que traten cuestiones de seguridad nacional y las actividades de tratamiento de datos personales que lleven a cabo los Estados miembros en el ejercicio de las actividades incluidas en el ámbito de aplicación del título V, capítulo 2, del Tratado de la Unión Europea (TUE).

(15) A fin de garantizar el mismo nivel de protección de las personas físicas a través de derechos jurídicamente exigibles en toda la Unión y evitar divergencias que dificulten el intercambio de datos personales entre las autoridades competentes, la presente Directiva debe establecer normas armonizadas para la protección y la libre circulación de los datos personales tratados con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública. La aproximación de las legislaciones de los Estados miembros no debe debilitar la protección de datos personales que ya se ofrece, sino que, por el contrario, debe tratar de garantizar un alto nivel de protección dentro de la Unión. No se debe impedir a los Estados miembros que ofrezcan garantías mayores que las establecidas en la presente Directiva para la protección de los derechos y libertades del interesado con respecto al tratamiento de sus datos personales por parte de las autoridades competentes.

(16) La presente Directiva se entiende sin perjuicio del principio de acceso del público a los documentos oficiales. Según el Reglamento (UE) 2016/679, los datos personales que figuran en documentos oficiales que se encuentren en posesión de una autoridad pública o de un organismo público o privado para la realización de una tarea de interés público pueden ser divulgados por dicha autoridad u organismo de conformidad con el Derecho de la Unión o del Estado miembro que resulte de aplicación a dicha autoridad u organismo público a fin de conciliar el derecho de acceso del público a los documentos oficiales con el derecho a la protección de los datos personales.

(17) La protección otorgada por la presente Directiva debe aplicarse a las personas físicas, independientemente de su nacionalidad o lugar de residencia, en lo que se refiere al tratamiento de sus datos personales.

(18) Para evitar que se produzcan graves riesgos de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de los datos personales, así como a su tratamiento manual si los datos personales están contenidos o destinados a ser incluidos en un fichero. Los ficheros o conjuntos de ficheros y sus portadas que no estén estructurados con arreglo a criterios específicos no deben incluirse en el ámbito de aplicación de la presente Directiva.

(19) El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo ([1]) se aplica al tratamiento de datos personales por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y los demás actos jurídicos de la Unión aplicables a ese tipo de tratamiento de datos personales deben adaptarse a los principios y normas establecidos en el Reglamento (UE) 2016/679.

(20) La presente Directiva no impide que, en las normas nacionales relativas a los procesos penales, los Estados miembros especifiquen operaciones y procedimientos de tratamiento relativos al tratamiento de datos personales por parte de tribunales y otras autoridades judiciales, en particular en lo que respecta a los datos personales contenidos en resoluciones judiciales o en registros relacionados con procesos penales.

([1]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

(21) Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Para determinar si una persona física es identificable deben tenerse en cuenta todos los medios con respecto a los cuales existe una probabilidad razonable de que puedan ser utilizados por el responsable del tratamiento o por cualquier otra persona para la identificación directa o indirecta de dicha persona física. Para determinar si existe una probabilidad razonable de que se utilicen unos medios determinados para la identificación de una persona física deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por tanto, los principios de protección de datos personales no deben aplicarse a la información anónima, a saber, información que no guarda relación con una persona física identificada o identificable, ni a los datos personales convertidos en anónimos de forma que el interesado al que se refieren ya no resulte identificable.

(22) Las autoridades públicas a las que se les faciliten datos personales en virtud de una obligación jurídica para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros, responsables de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las autoridades públicas siempre deben solicitar los datos por escrito, de forma justificada y con carácter ocasional, y los datos solicitados no podrán referirse a la totalidad de un fichero o suponer la interconexión de varios ficheros. El tratamiento de datos personales por las citadas autoridades públicas debe estar en consonancia con la normativa en materia de protección de datos que resulte de aplicación en función de la finalidad del tratamiento.

(23) Debe entenderse por datos genéticos todos los datos personales relacionados con las características genéticas de una persona física que se hayan heredado o adquirido y que aporten información única sobre la fisiología o la salud de esa persona física, y que resultan de análisis de una muestra biológica de la persona física de que se trate, en particular cromosómicos, del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o de análisis de cualquier otro elemento que permita obtener información equivalente. Habida cuenta de la complejidad y la sensibilidad de la información genética, existe un alto riesgo de que el responsable del tratamiento haga un uso indebido de la misma o la reutilice con fines no autorizados. Toda discriminación por razón de características genéticas debe quedar prohibida con carácter general.

(24) Entre los datos personales relacionados con la salud se deberían incluir todos los datos relativos al estado de salud del interesado que revelen información relativa al estado de la salud física o mental pasado, presente o futuro del interesado, incluidos los datos personales recopilados durante la inscripción de una persona física a efectos de la prestación de servicios de asistencia sanitaria a dicha persona o durante la prestación de tales servicios, de conformidad con lo dispuesto en la Directiva 2011/24/UE del Parlamento Europeo y del Consejo ([1]); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluidos los datos genéticos y las muestras biológicas, y cualquier información relativa, por ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, ya sea un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro, por ejemplo.

(25) Todos los Estados miembros están afiliados a la Organización Internacional de Policía Criminal (Interpol). Para cumplir su misión, Interpol recibe, almacena y distribuye datos personales para ayudar a las autoridades competentes a prevenir y combatir la delincuencia internacional. Por ello, conviene reforzar la cooperación entre la Unión e Interpol facilitando un intercambio eficaz de datos personales, a la vez que se garantiza el respeto de los derechos y libertades fundamentales en relación con el tratamiento automatizado de los datos personales. Cuando se transmitan datos desde la Unión a Interpol y a los países que hayan destinado miembros a dicha organización, resultará de aplicación la presente Directiva, en particular lo dispuesto en materia de transmisiones internacionales de datos. La presente Directiva se entenderá sin perjuicio de las normas específicas establecidas en la Posición Común 2005/69/JAI del Consejo ([2]) y en la Decisión 2007/533/JAI del Consejo ([3]).

(26) Todo tratamiento de datos personales debe ser lícito, leal y transparente en relación con las personas físicas afectadas, y únicamente podrá llevarse a cabo con los fines específicos previstos en la ley. Ello no impide, *per se*, que las autoridades policiales puedan llevar a cabo actividades tales como las investigaciones encubiertas o la videovigilancia. Tales actividades pueden realizarse con fines de prevención, investigación, detección o

([1]) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

([2]) Posición Común 2005/69/JAI del Consejo, de 24 de enero de 2005, relativa al intercambio de determinados datos con Interpol (DO L 27 de 29.1.2005, p. 61).

([3]) Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 205 de 7.8.2007, p. 63).

enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas para la seguridad pública, siempre y cuando estén previstas en la legislación y constituyan una medida necesaria y proporcionada en una sociedad democrática, con el debido respeto a los intereses legítimos de la persona física afectada. El principio de tratamiento leal en materia de protección de datos es un concepto distinto del derecho a un «juicio imparcial», según se define en el artículo 47 de la Carta y en el artículo 6 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en lo sucesivo, «CEDH»). Debe informarse a las personas físicas de los riesgos, reglas, salvaguardias y derechos aplicables en relación con el tratamiento de sus datos personales, así como del modo de hacer valer sus derechos en relación con dicho tratamiento. En particular, los fines específicos a los que obedezca el tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de la recopilación de los datos personales. Los datos personales deben ser adecuados y pertinentes en relación con los fines para los que se tratan, lo cual requiere, en particular, que se garantice que los datos personales recogidos no son excesivos ni se conservan más tiempo del que sea necesario para los fines con los que se tratan. Los datos personales solo deberían ser objeto de tratamiento si la finalidad del tratamiento no puede lograrse razonablemente por otros medios. Para garantizar que los datos no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su eliminación o revisión periódica. Los Estados miembros deben establecer las salvaguardias adecuadas en relación con los datos personales almacenados por períodos más largos para su archivo por cuestiones de interés público o para su uso científico, estadístico o histórico.

(27) Para la prevención, investigación y enjuiciamiento de las infracciones penales, es necesario que las autoridades competentes traten datos personales recopilados en el contexto de la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales concretas más allá de ese contexto específico, con el fin de adquirir un mejor conocimiento de las actividades delictivas y establecer vínculos entre las distintas infracciones penales detectadas.

(28) Con el fin de mantener la seguridad del tratamiento y evitar que con él se infrinja lo dispuesto en la presente Directiva, los datos personales deben ser tratados de modo que se garantice un nivel adecuado de seguridad y confidencialidad, en particular impidiendo el acceso sin autorización a dichos datos o el uso no autorizado de los mismos y del equipo utilizado en el tratamiento, teniendo en cuenta el desarrollo técnico existente y la tecnología, los costes de ejecución con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

(29) Los datos personales deben recogerse con fines determinados, explícitos y legítimos dentro del ámbito de aplicación de la presente Directiva y no deben ser tratados para fines incompatibles con los fines de la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública. Si el mismo u otro responsable del tratamiento trata datos personales con alguno de los fines previstos en el ámbito de aplicación de la presente Directiva distinto del fin para el que los datos fueron recopilados, dicho tratamiento debe permitirse con la condición de que el mismo esté autorizado con arreglo a la legislación aplicable y sea necesario y proporcionado para dicho otro fin.

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

(31) Es inherente al tratamiento de datos personales en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se traten datos personales relativos a diferentes categorías de interesados. Por ello, si procede y siempre que sea posible, se deben diferenciar claramente los datos personales de distintas categorías de interesados, tales como los sospechosos, los condenados por una infracción penal, las víctimas o los terceros, entre los que se incluyen los testigos, las personas que posean información o contactos útiles y los cómplices de sospechosos y delincuentes condenados. Lo anterior no debe impedir la aplicación del derecho a la presunción de inocencia tal como lo garantiza la Carta y el CEDH, según los ha interpretado la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos, respectivamente.

(32) Las autoridades competentes deben velar por que los datos personales que sean inexactos, incompletos o que no estén actualizados no se transmitan ni estén disponibles. Con el fin de garantizar tanto la protección de las personas físicas como la exactitud, integridad, actualidad y fiabilidad de los datos personales que se transmitan o se pongan a disposición de terceros, las autoridades competentes deben, en la medida de lo posible, añadir la información necesaria a todos los datos personales que transmitan.

(33) Las referencias de la presente Directiva al Derecho de un Estado miembro, a una base jurídica o a una medida legislativa no requieren necesariamente la existencia de un acto legislativo adoptado por un Parlamento, sin

perjuicio de los requisitos exigidos por el ordenamiento constitucional del Estado miembro de que se trate. No obstante, dicho Derecho de un Estado miembro, base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para quienes estén sujetos a la misma, tal y como exige la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos. Cuando en el Derecho de un Estado miembro se regule el tratamiento de los datos personales dentro del ámbito de aplicación de la presente Directiva, se deben indicar al menos los objetivos del tratamiento, los datos personales que serán objeto del mismo, la finalidad del tratamiento, los procedimientos para el mantenimiento de la integridad y la confidencialidad de los datos personales y los procedimientos para su destrucción, proporcionando con ello garantías suficientes frente a los riesgos de abuso y arbitrariedad.

(34) El tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a amenazas para la seguridad pública, debe abarcar toda operación o conjunto de operaciones con datos personales o conjuntos de datos personales que se lleve a cabo con tales fines, ya sea de modo automatizado o no, y entre las que se incluye la recopilación, registro, organización, estructuración, almacenamiento, adaptación o modificación, recuperación, consulta, utilización, cotejo o combinación, limitación del tratamiento, supresión o destrucción de datos. En particular, las normas de la presente Directiva deben aplicarse a la transmisión de datos personales a los efectos de la presente Directiva a un destinatario que no esté sometido a la misma. Por «destinatario» debe entenderse toda persona física o jurídica, autoridad pública, servicio u otro organismo al que la autoridad competente comunique los datos personales de forma lícita. Si los datos personales fueron recopilados inicialmente por una autoridad competente para alguno de los fines previstos en la presente Directiva, el tratamiento de dichos datos para fines distintos de los previstos en la presente Directiva se regirá por lo dispuesto en el Reglamento (UE) 2016/679, siempre que dicho tratamiento esté autorizado por el Derecho de la Unión o del Estado miembro. En particular, las normas del Reglamento (UE) 2016/679 deben aplicarse a la transmisión de datos personales con fines no previstos en el ámbito de aplicación de la presente Directiva. Para el tratamiento de datos personales por parte de un destinatario que no sea una autoridad competente o que esté actuando como tal en el sentido de la presente Directiva y a quien una autoridad competente haya comunicado datos personales lícitamente, se estará a lo dispuesto en el Reglamento (UE) 2016/679. Al aplicar la presente Directiva, los Estados miembros deben poder precisar también la aplicación de las normas del Reglamento (UE) 2016/679, con sujeción a las condiciones establecidas en el mismo.

(35) Para que sea lícito, el tratamiento de datos personales en virtud de la presente Directiva debe ser necesario para el desempeño de una función de interés público llevada a cabo por una autoridad competente en virtud del Derecho de la Unión o de un Estado miembro con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública. Entre tales actividades debe incluirse la protección de los intereses vitales del interesado. El ejercicio de las funciones de prevención, investigación, detección o enjuiciamiento de infracciones penales que la legislación atribuye institucionalmente a las autoridades competentes permite a estas exigir u ordenar a las personas físicas que atiendan a las solicitudes que se les dirijan. En este caso, el consentimiento del interesado [según se define en el Reglamento (UE) 2016/679] no constituye un fundamento jurídico para el tratamiento de los datos personales por las autoridades competentes. Cuando se exige al interesado que cumpla una obligación jurídica, este no goza de verdadera libertad de elección, por lo que no puede considerarse que su respuesta constituya una manifestación libre de su voluntad. Ello no debe ser óbice para que los Estados miembros establezcan en su legislación la posibilidad de que el interesado pueda aceptar el tratamiento de sus datos personales a los efectos de la presente Directiva, por ejemplo, para la realización de pruebas de ADN en las investigaciones penales o el control del paradero del interesado mediante dispositivos electrónicos para la ejecución de sanciones penales.

(36) Los Estados miembros deben establecer que, cuando el Derecho de la Unión o de los Estados miembros que sean de aplicación a la autoridad transmisora competente dispongan la aplicación de condiciones específicas al tratamiento de datos personales en circunstancias específicas (como el uso de códigos de tratamiento), la autoridad transmisora competente debe informar de dichas condiciones y de la obligación de respetarlas al destinatario al que se transmiten los datos. Tales condiciones pueden incluir, por ejemplo, la prohibición de transmitir los datos personales a otros o utilizarlos para otros fines distintos de aquellos para los que fueron transmitidos al destinatario, o, en caso de limitación del derecho de información, la prohibición de que dicho destinatario informe al interesado sin la autorización previa de la autoridad transmisora competente. Dichas obligaciones también resultan de aplicación a las transmisiones de datos por parte de la autoridad transmisora competente a destinatarios de terceros países u organizaciones internacionales. Los Estados miembros deben establecer que la citada autoridad competente no aplique a los destinatarios de otros Estados miembros o a los órganos y organismos establecidos en virtud de la tercera parte, título V, capítulos 4 y 5, del TFUE condiciones distintas de las aplicables a las transmisiones de datos similares que tengan lugar dentro del Estado miembro de la autoridad transmisora competente.

(37) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento puede generar riesgos importantes para los derechos y las libertades fundamentales. Dichos datos personales deben incluir aquellos que pongan de manifiesto el origen racial o étnico, entendiéndose que el término «origen racial»

empleado en la presente Directiva no implica la aceptación por parte de la Unión Europea de teorías que traten de determinar la existencia de razas humanas diferentes. Tales datos personales no deben ser objeto de tratamiento, salvo que el tratamiento esté supeditado a las garantías adecuadas de protección de los derechos y libertades del interesado que se establecen en la legislación y esté permitido en los casos autorizados por la ley; o, si no está ya autorizado por dicha legislación, que el tratamiento sea necesario para proteger los intereses vitales del interesado o de otra persona, o que el tratamiento se refiera a datos que el interesado ya ha hecho públicos de forma manifiesta. Entre las garantías adecuadas de protección de los derechos y libertades del interesado pueden figurar, por ejemplo, la posibilidad de recopilar tales datos únicamente en relación con otros datos de la persona física afectada, la posibilidad de proteger adecuadamente los datos recopilados, el establecimiento de normas más estrictas para el acceso a los datos por parte del personal de la autoridad competente, o la prohibición de transmisión de dichos datos. El tratamiento de este tipo de datos también debe estar jurídicamente permitido si el interesado ha acordado de forma explícita que el tratamiento de los datos resulte especialmente intrusivo para las personas. Sin embargo, el consentimiento del interesado no debe constituir en sí mismo un fundamento jurídico para que las autoridades competentes procedan al tratamiento de datos personales sensibles como los mencionados.

(38) El interesado debe tener derecho a no ser objeto de una decisión que evalúe aspectos personales que le conciernen que se base únicamente en un tratamiento automatizado de los datos y que tenga efectos jurídicos adversos que le conciernan o le afecten significativamente. En todo caso, este tipo de tratamiento debe estar sujeto a las garantías apropiadas, lo que incluye informar de forma específica al interesado, así como el derecho a la intervención humana, en particular para que el interesado pueda expresar su punto de vista, obtener una explicación de la decisión adoptada tras dicha evaluación, o ejercer su derecho a impugnar la decisión. Queda prohibida la elaboración de perfiles que dé lugar a la discriminación de personas físicas por razones basadas en datos personales que, por su naturaleza, son especialmente sensibles en relación con los derechos y las libertades fundamentales, con arreglo a las condiciones previstas en los artículos 21 y 52 de la Carta.

(39) Para poder ejercer sus derechos, toda la información dirigida al interesado debe ser fácilmente accesible, en particular, en el sitio web del responsable del tratamiento, y fácil de entender, para lo que debe emplearse un lenguaje claro y sencillo. Dicha información debe adaptarse a las necesidades de las personas vulnerables, entre las que se incluyen los niños.

(40) Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos con arreglo a las disposiciones adoptadas de conformidad con la presente Directiva, incluidos mecanismos para solicitar y, en su caso, obtener, de forma gratuita, el acceso a sus datos personales, así como su rectificación o supresión y la limitación de su tratamiento. El responsable del tratamiento debe estar obligado a responder sin dilación indebida a las solicitudes del interesado, salvo que aplique restricciones a los derechos del interesado de conformidad con la presente Directiva. Asimismo, si las solicitudes son manifiestamente infundadas o excesivas, como cuando el interesado solicita información de forma poco razonable y repetitiva o abusa de su derecho a recibir información, por ejemplo proporcionando información falsa o engañosa al presentar la solicitud, el responsable del tratamiento debe ser capaz de exigir el pago de un canon razonable o negarse a dar curso a la solicitud.

(41) Cuando el responsable del tratamiento solicite información complementaria que resulte necesaria para confirmar la identidad del interesado, dicha información debe tratarse únicamente a tal efecto y no debe almacenarse más tiempo del que sea necesario para dicho fin.

(42) Debe informarse al interesado, como mínimo, de lo siguiente: la identidad del responsable del tratamiento, la existencia de la operación de tratamiento, los fines del tratamiento, el derecho a presentar una reclamación y el derecho a solicitar al responsable del tratamiento el acceso a los datos personales, su rectificación o supresión, o la limitación de su tratamiento. Esta información se podrá facilitar en el sitio web de la autoridad competente. Además, en determinados casos y con el fin de permitir que ejerza sus derechos, debe informarse al interesado de la base jurídica en la que se fundamenta el tratamiento y del período durante el que se conservarán los datos, siempre que dicha información adicional resulte necesaria y habida cuenta de las circunstancias concretas en que se produce el tratamiento de los datos, a fin de garantizar un tratamiento leal en lo que respecta al interesado.

(43) Toda persona física debe tener derecho a acceder a los datos que se hayan recopilado en relación con ella y a poder ejercer este derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Todo interesado debe, por tanto, tener derecho a conocer y a que se le comuniquen, en particular, la finalidad del tratamiento, el plazo de conservación de los datos y los destinatarios que los reciben, incluso en terceros países. Cuando esta comunicación incluya información relativa al origen de los datos personales, dicha información no debe revelar la identidad de ninguna persona física, sobre todo cuando se trate de fuentes confidenciales. Para que se considere que se ha respetado ese derecho, basta con que el interesado esté en posesión de un resumen completo de tales datos presentados de forma inteligible, es decir, de forma que el interesado pueda tener conocimiento de los mismos y verificar que son exactos y que su tratamiento se ha

realizado de conformidad con la presente Directiva, de modo que, si ha lugar, pueda ejercer los derechos que esta le confiere. Dicho resumen puede ser una copia de los datos personales que están siendo objeto de tratamiento.

(44) Debe permitirse a los Estados miembros adoptar medidas legislativas que retrasen, limiten u omitan que se facilite información a los interesados o que limiten, total o parcialmente, el acceso de los interesados a sus datos personales, en la medida en que dichas medidas sean necesarias y proporcionadas en una sociedad democrática y mientras sigan siéndolo, con el debido respeto a los derechos fundamentales y los intereses legítimos de la persona física afectada, con el fin de no entorpecer las indagaciones, investigaciones o procedimientos oficiales o judiciales, de no perjudicar la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, de proteger la seguridad pública o la seguridad nacional o de salvaguardar los derechos y las libertades de terceros. El responsable del tratamiento debe evaluar, mediante un análisis individual y específico de cada caso, si procede o no restringir, total o parcialmente, el derecho de acceso.

(45) Toda denegación o restricción de acceso debe, en principio, comunicarse por escrito al interesado precisando los fundamentos de hecho o de Derecho en los que se basa la decisión.

(46) Toda restricción de los derechos del interesado debe cumplir con lo dispuesto en la Carta y el CEDH, según los ha interpretado la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos, respectivamente, y, en particular, respetar el contenido esencial de los citados derechos y libertades.

(47) Toda persona física debe tener derecho a la rectificación de aquellos datos personales inexactos que le conciernan, en particular cuando estén relacionados con hechos, así como a la supresión de los datos cuyo tratamiento no se ajuste a lo dispuesto en la presente Directiva. Sin embargo, el derecho de rectificación no debe afectar, por ejemplo, al contenido de la declaración de un testigo. Asimismo, toda persona física debe tener derecho a la limitación del tratamiento cuando, tras impugnar la exactitud de un dato de carácter personal, no sea posible determinar su exactitud o inexactitud, o cuando los datos personales deban conservarse a efectos probatorios. En particular, en lugar de suprimir los datos personales, el tratamiento debe limitarse si en un caso concreto hay razones justificadas para suponer que la supresión podría perjudicar los intereses legítimos del interesado. En tal caso, los datos restringidos podrán tratarse únicamente para los fines que impidieron su supresión. Entre los métodos para limitar el tratamiento de datos personales podrían incluirse, entre otros, los consistentes en trasladar los datos seleccionados a otro sistema de tratamiento, por ejemplo a efectos de archivo, o en impedir el acceso a los datos seleccionados. En los ficheros automatizados, la limitación del tratamiento de datos personales debe hacerse, en principio, por medios técnicos; la limitación del tratamiento de los datos personales debe indicarse en el sistema de tal modo que quede claro que el tratamiento de los datos personales está limitado. Debe notificarse a los destinatarios a los que se hayan comunicado los datos inexactos y a las autoridades competentes de las que procedan dichos datos inexactos que se ha procedido a rectificar o suprimir los datos personales o a limitar su tratamiento. Los responsables del tratamiento deben abstenerse asimismo de toda divulgación ulterior de los citados datos.

(48) Si el responsable del tratamiento deniega al interesado sus derechos de información, acceso a los datos personales, o rectificación o supresión de estos, o la limitación de su tratamiento, el interesado debe tener derecho a solicitar que la autoridad nacional de control verifique la licitud del tratamiento. El interesado debe ser informado de este derecho. Cuando actúe por cuenta del interesado, la autoridad de control debe informarle, como mínimo, de que ha llevado a cabo todas las verificaciones o revisiones necesarias. La autoridad de control también debe informar al interesado de su derecho a la tutela judicial.

(49) Cuando los datos personales sean tratados en el transcurso de una investigación penal o un procedimiento judicial en materia penal, el ejercicio de los derechos de información, acceso a los datos personales, rectificación o supresión de estos y la limitación de su tratamiento podrá ejercerse de conformidad con el Derecho procesal nacional.

(50) Se debe establecer la responsabilidad del responsable del tratamiento en relación con cualquier tratamiento de datos personales realizado por él mismo o en su nombre. En particular, el responsable del tratamiento debe estar obligado a poner en marcha medidas oportunas y eficaces y a poder demostrar la conformidad de las actividades de tratamiento con la presente Directiva. Estas medidas deben tener en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo que representan para los derechos y las libertades de las personas físicas. Las medidas adoptadas por el responsable del tratamiento deben incluir la formulación y puesta en marcha de salvaguardias específicas en relación con el tratamiento de los datos personales de personas físicas vulnerables, en particular los niños.

(51) Los riesgos para los derechos y libertades de los interesados, de diversa probabilidad y gravedad, pueden producirse debido a un tratamiento de datos capaz de provocar daños físicos, materiales o inmateriales, en particular cuando el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas económicas, menoscabo de la reputación, pérdida de confidencialidad de datos sujetos al secreto

profesional, inversión no autorizada de la seudonimización, o cualquier otro perjuicio económico o social significativo; cuando los interesados se vean privados de sus derechos y libertades o de la posibilidad de ejercer el control sobre sus datos personales; cuando los datos personales tratados pongan de manifiesto el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, cuando se traten datos genéticos o datos biométricos que permiten la identificación unívoca de una persona o cuando se traten datos relativos a la salud o a la vida y orientación sexuales o a los antecedentes e infracciones penales u otras medidas de seguridad relacionadas; cuando se evalúen aspectos personales, en particular en el marco del análisis y la predicción de aspectos referidos al rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la ubicación o los movimientos, con el fin de crear o utilizar perfiles personales; cuando se traten datos personales de personas físicas vulnerables, en particular los niños; o cuando el tratamiento se refiera a una gran cantidad de datos personales y afecte a un elevado número de interesados.

(52) La probabilidad y la gravedad del riesgo debe determinarse en función de la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe determinarse basándose en una evaluación objetiva, mediante la cual se determine si las operaciones de tratamiento de datos suponen un alto riesgo. Un alto riesgo es un especial riesgo de perjuicio para los derechos y libertades de los interesados.

(53) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de las oportunas medidas de carácter técnico y organizativo con el fin de garantizar el cumplimiento de lo dispuesto en la presente Directiva. La aplicación de tales medidas no puede depender únicamente de criterios económicos. A fin de poder demostrar que cumple lo dispuesto en la presente Directiva, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que respeten, en particular, los principios de la protección de datos desde la concepción y de la protección de datos por defecto. Cuando el responsable del tratamiento haya llevado a cabo una evaluación de impacto relativa a la protección de datos con arreglo a lo dispuesto en la presente Directiva, los resultados de dicha evaluación se deben tener en cuenta en la formulación de tales medidas y procedimientos. Dichas medidas pueden consistir, entre otras cosas, en la utilización, lo antes posible, de procesos de seudonimización. El uso de la seudonimización a los efectos de la presente Directiva puede contribuir, en particular, a la libre circulación de datos personales dentro del espacio de libertad, seguridad y justicia.

(54) La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud de la presente Directiva, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables del tratamiento o en los que el tratamiento se lleve a cabo por cuenta de otro responsable.

(55) La realización del tratamiento por un encargado del tratamiento debe regirse por un acto jurídico, en particular, un contrato que obligue al encargado frente al responsable del tratamiento y que estipule, concretamente, que el encargado debe actuar únicamente con arreglo a las instrucciones del responsable. El encargado del tratamiento debe tener en cuenta los principios de la protección de datos desde la concepción y de la protección de datos por defecto.

(56) Para demostrar que se cumple lo dispuesto en la presente Directiva, el responsable o el encargado del tratamiento debe mantener registros relativos a todas las categorías de actividades de tratamiento que se lleven a cabo bajo su responsabilidad. Todos los responsables y todos los encargados del tratamiento deben estar obligados a cooperar con la autoridad de control y a poner dichos registros a su disposición, cuando lo solicite, de modo que puedan servir para supervisar las operaciones de tratamiento. Los responsables o los encargados del tratamiento que traten datos personales mediante sistemas de tratamiento no automatizado deben contar con métodos eficaces, como los registros diarios o de otro tipo, para demostrar la licitud del tratamiento, permitir el autocontrol y garantizar la integridad y la seguridad de los datos.

(57) Deben conservarse registros, como mínimo, de las operaciones llevadas a cabo mediante sistemas de tratamiento automatizado, entre las que se incluyen la recopilación, la modificación, la consulta, la comunicación (incluida la transmisión), la combinación o la supresión de datos. Los datos identificativos de la persona que consulta o comunica los datos personales deben quedar registrados y, a partir de dichos datos, debe ser posible establecer la justificación de las operaciones de tratamiento. Los registros se deben utilizar únicamente para comprobar la licitud del tratamiento de datos, a efectos de autocontrol y para garantizar la integridad y la seguridad de los datos y los procesos penales. El autocontrol abarca, asimismo, los procedimientos disciplinarios en el seno de las autoridades competentes.

(58) El responsable del tratamiento debe realizar una evaluación del impacto sobre la protección de datos cuando exista la probabilidad de que, por su naturaleza, alcance o fines, las operaciones de tratamiento entrañen un alto riesgo para los derechos y las libertades de los interesados; dicha evaluación debe incluir, en particular, las medidas, garantías y mecanismos previstos para garantizar la protección de los datos personales y demostrar la conformidad con la presente Directiva. Las evaluaciones de impacto deben abarcar los sistemas y procesos correspondientes de las operaciones de tratamiento, pero no harán referencia a casos concretos.

(59) Con el fin de garantizar la protección efectiva de los derechos y las libertades de los interesados, en determinados casos, el responsable o el encargado del tratamiento debe consultar a la autoridad de control antes del tratamiento previsto.

(60) Al objeto de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en la presente Directiva, el responsable o el encargado del tratamiento deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica, el coste de su aplicación con respecto al riesgo y la naturaleza de los datos personales que deban protegerse. En la evaluación de los riesgos relacionados con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos, como la destrucción accidental o ilícita, la pérdida, la alteración, la comunicación no autorizada o el acceso no autorizado a datos personales transmitidos, almacenados o sometidos a cualquier otro tipo de tratamiento, que puedan ocasionar, en particular, perjuicios físicos, materiales o inmateriales. El responsable y el encargado del tratamiento deben asegurarse de que el tratamiento de datos personales no lo llevan a cabo personas no autorizadas.

(61) Si no se toman medidas adecuadas de manera adecuada y oportuna, las violaciones de la seguridad de datos personales pueden dar lugar a daños y perjuicios físicos, materiales o inmateriales para las personas físicas, entre los que se incluyen la pérdida de control sobre sus datos personales o la restricción de sus derechos, la discriminación, la usurpación de la identidad, las pérdidas financieras, la inversión no autorizada de una seudonimización, el menoscabo de la reputación, la pérdida de confidencialidad de datos personales sujetos al secreto profesional o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por ello, en cuanto el responsable del tratamiento tenga conocimiento de que se ha producido una violación de datos personales, debe notificarlo sin dilación indebida a la autoridad de control y, cuando sea factible, en el plazo de 72 horas después de haberlo sabido, a menos que el responsable del tratamiento pueda demostrar, de conformidad con el principio de rendición de cuentas, que es improbable que dicha violación entrañe un riesgo para los derechos y las libertades de las personas físicas. Cuando no sea posible efectuar la notificación en el plazo de 72 horas, esta debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse la información por fases sin más dilaciones indebidas.

(62) Se debe informar a las personas físicas sin dilación indebida en el supuesto de que sea probable que la violación de la seguridad de datos personales entrañe un alto riesgo para sus derechos y libertades, a fin de que puedan adoptar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de datos personales e incluir recomendaciones para que la persona física afectada mitigue los posibles efectos adversos. Las comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible, en estrecha cooperación con la autoridad de control y siguiendo sus directrices o las establecidas por otras autoridades competentes. Así, por ejemplo, la necesidad de mitigar un riesgo inmediato de perjuicio habría que comunicarla a los interesados de forma inmediata, mientras que la necesidad de aplicar medidas adecuadas para impedir que se sigan violando los datos o se produzcan violaciones de la seguridad de datos similares puede justificar más tiempo para la comunicación. Cuando el hecho de retrasar o restringir la comunicación de una violación de la seguridad de datos personales a la persona física afectada no sea suficiente para evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales, evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales, proteger la seguridad pública o la seguridad nacional o proteger los derechos y libertades de otras personas, dicha comunicación, en circunstancias excepcionales, podrá omitirse.

(63) El responsable del tratamiento designará a una persona para que le asista en la supervisión del cumplimiento interno de las disposiciones adoptadas en virtud de la presente Directiva, salvo en los casos en los que un Estado miembro decida eximir a los órganos jurisdiccionales y demás autoridades judiciales independientes cuando actúen en el ejercicio de su función jurisdiccional. Dicha persona podrá ser un empleado que ya trabaje para el responsable del tratamiento y que haya recibido una formación especial sobre la legislación y las prácticas de protección de datos, con el fin de adquirir conocimientos especializados en este ámbito. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función del tratamiento de datos que se lleve a cabo y de la protección exigida para los datos personales tratados por el responsable del tratamiento. Podrá desempeñar sus funciones a tiempo completo o a tiempo parcial. Varios responsables del tratamiento podrán nombrar conjuntamente a un mismo delegado de protección de datos teniendo en cuenta su estructura organizativa y tamaño, como, por ejemplo, en el caso de que compartan recursos en unidades centralizadas. Dicha persona también podrá ser designada para ocupar otros cargos dentro de la estructura organizativa de los responsables del tratamiento en cuestión. Debe prestar ayuda al responsable del tratamiento y a los empleados que lleven a cabo el tratamiento de datos personales facilitándoles información y asesoramiento sobre el cumplimiento de las obligaciones que les correspondan en materia de protección de datos. Tales delegados de protección de datos deben estar en condiciones de desempeñar sus deberes y funciones con independencia y de conformidad con el Derecho del Estado miembro.

(64) Los Estados miembros deben velar por que las transferencias de datos a terceros países o a organizaciones internacionales solo se lleven a cabo si resultan necesarias para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y la prevención frente

a las amenazas para la seguridad pública, y si el responsable del tratamiento en el tercer país u organización internacional de que se trate es una autoridad competente en el sentido de lo dispuesto en la presente Directiva. Las transferencias de datos solo pueden llevarlas a cabo las autoridades competentes cuando actúen en calidad de responsables del tratamiento, salvo que los encargados del tratamiento hayan recibido instrucciones expresas de llevar a cabo la transferencia en nombre de los responsables del tratamiento. Dichas transferencias pueden tener lugar en los casos en que la Comisión haya decidido que el tercer país o la organización internacional en cuestión garantizan un nivel adecuado de protección, o cuando se hayan ofrecido unas garantías apropiadas o se apliquen excepciones para situaciones específicas. Cuando los datos personales sean transferidos desde la Unión a responsables y encargados del tratamiento u otros destinatarios de terceros países u organizaciones internacionales, no debe verse menoscabado el nivel de protección de las personas físicas que se garantiza en la Unión mediante la presente Directiva, ni tampoco en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados del tratamiento del mismo u otro tercer país u organización internacional.

(65) Cuando los datos personales se transfieran de un Estado miembro a terceros países u organizaciones internacionales, dicha transferencia solo debe realizarse, en principio, después de que el Estado miembro del que se obtuvieron los datos haya autorizado la transferencia. A los efectos de una cooperación eficaz en materia policial, es necesario que, cuando la naturaleza de una amenaza para la seguridad pública de un Estado miembro o de un tercer país o para los intereses fundamentales de un Estado miembro sea tan inmediata como para que resulte imposible conseguir la autorización previa a tiempo, la autoridad competente debe poder transferir los datos personales de que se trate al tercer país u organización internacional correspondiente sin dicha autorización previa. Los Estados miembros deben disponer que se comuniquen al tercer país y/o a la organización internacional que corresponda todas las condiciones específicas aplicables a la transferencia. Toda transferencia ulterior de datos personales estará supeditada a la autorización previa de la autoridad competente que llevó a cabo la transferencia inicial. Al decidir si autorizar dicha transferencia ulterior de los datos, la autoridad competente que llevó a cabo la transferencia inicial debe tener debidamente en cuenta todos los factores pertinentes, entre los que se incluye la gravedad de la infracción penal, las condiciones específicas de la transferencia y la finalidad para la que se transfirieron los datos en primera instancia, la naturaleza y las condiciones de ejecución de la sanción penal y el nivel de protección de datos personales existente en el tercer país o la organización internacional a los que se van a transferir los datos. La autoridad competente que llevó a cabo la transferencia inicial también podrá supeditar la transferencia ulterior de los datos a condiciones específicas. Dichas condiciones específicas se pueden describir, por ejemplo, mediante el empleo de códigos de tratamiento.

(66) La Comisión debe poder decidir, con efectos para toda la Unión, que determinados terceros países, o un territorio, o uno o más sectores específicos de 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 ofrecen tal nivel de protección. En estos casos, se podrán efectuar transferencias de datos personales a tales países sin necesidad de obtener una autorización específica, salvo que otro Estado miembro, del que se hayan obtenido los datos, tenga que autorizar la transferencia.

(67) 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 de un tercer país, de un territorio, o de un sector específico de un tercer país, debe tener en cuenta la medida en que dicho tercer país respeta el Estado de Derecho, el acceso a la justicia y las normas y principios internacionales en materia de derechos humanos, y su Derecho tanto general como sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el Derecho penal y el orden público. En la adopción de una decisión de adecuación en relación con un territorio o un sector específico de un tercer país, se deben tener en cuenta criterios claros y objetivos, como las actividades de tratamiento concretas y el ámbito de aplicación de las normas jurídicas y la legislación vigentes en el tercer país. El tercer país en cuestión debe ofrecer garantías que aseguren un nivel de protección adecuado que sea esencialmente equivalente al garantizado en el interior de la Unión, en particular cuando los datos se sometan a tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar la supervisión eficaz e independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, y ofrecer a los interesados derechos efectivos y exigibles, así como un derecho a la tutela administrativa y judicial efectiva.

(68) Aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión también debe tener en cuenta las obligaciones resultantes de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de las citadas obligaciones. En particular, debería tenerse en cuenta la adhesión del país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos personales y su Protocolo adicional. La Comisión debe

consultar al Comité Europeo de Protección de Datos establecido por el Reglamento (UE) 2016/679 al evaluar el nivel de protección existente en terceros países u organizaciones internacionales. La Comisión también debe tener en cuenta las decisiones de adecuación que haya adoptado de conformidad con el artículo 45 del Reglamento (UE) 2016/679.

(69) La Comisión debe supervisar el funcionamiento de las decisiones relativas al nivel de protección de un tercer país, territorio o sector específico de un tercer país, o de una organización internacional. En sus decisiones de adecuación, la Comisión debe establecer un mecanismo para la revisión periódica de su funcionamiento. Esta revisión periódica debe realizarse en colaboración con el tercer país u organización internacional de que se trate y debe tener en cuenta todas las novedades pertinentes que se produzcan en dicho tercer país u organización internacional.

(70) La Comisión también debe poder determinar que un tercer país, un territorio, un sector específico de un tercer país o una organización internacional han dejado de garantizar un nivel adecuado de protección de datos. En tal caso, debe prohibirse la transferencia de datos personales a dicho tercer país u organización internacional, salvo que se cumplan los requisitos de la presente Directiva relativos a las transferencias sujetas a garantías y excepciones adecuadas para situaciones particulares. Deben establecerse los procedimientos para la celebración de consultas entre la Comisión y dichos terceros países u organizaciones internacionales. La Comisión debe informar oportunamente al tercer país u organización internacional de las razones de la situación y entablar consultas a fin de subsanarla.

(71) Las transferencias no basadas en tales decisiones de adecuación solo deben permitirse cuando se hayan ofrecido las garantías adecuadas en un instrumento jurídicamente vinculante que aseguren la protección de los datos personales o cuando el responsable del tratamiento haya evaluado todas las circunstancias de la transferencia de datos y, sobre la base de tal evaluación, considere que se dan las garantías adecuadas con respecto a la protección de los datos personales. Tales instrumentos jurídicamente vinculantes podrían ser, por ejemplo, acuerdos bilaterales jurídicamente vinculantes celebrados por los Estados miembros y aplicados en su ordenamiento jurídico y cuyo cumplimiento pueda ser exigido por los interesados de dichos Estados, de forma que se garantice el cumplimento de los requisitos de protección de datos y el respeto de los derechos de los interesados, entre los que se incluye el derecho a la tutela administrativa o judicial efectiva. El responsable del tratamiento puede tener en cuenta los acuerdos de cooperación celebrados entre Europol o Eurojust y terceros países que permitan el intercambio de datos personales al llevar a cabo la evaluación de todas las circunstancias que concurran en la transferencia de datos. El responsable del tratamiento también puede tener en cuenta si la transferencia de datos va a estar sujeta a obligaciones de confidencialidad y al principio de especificidad, que garantiza que los datos no se tratarán para fines distintos de aquellos para los que se han transferido. Además, el responsable del tratamiento debe verificar que los datos personales no vayan a ser utilizados para solicitar, dictar o ejecutar la pena capital u otra forma de trato cruel o inhumano. Aunque estas condiciones puedan considerarse protecciones adecuadas que permitan la trasferencia de los datos, el responsable del tratamiento podrá exigir salvaguardias adicionales.

(72) De no existir ni una decisión de adecuación ni unas garantías adecuadas, únicamente podrá realizarse una transferencia de datos o una categoría de transferencias de datos en situaciones específicas, y si fuera necesario, a fin de proteger los intereses vitales del interesado o de otra persona, o de proteger los intereses legítimos del interesado cuando así lo disponga la legislación del Estado miembro que transfiere los datos personales, para prevenir una amenaza inmediata y grave para la seguridad pública de un Estado miembro o de un tercer país, en un caso concreto a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a amenazas para la seguridad pública, o en un caso concreto para el reconocimiento, el ejercicio o la defensa de una pretensión jurídica. Dichas excepciones se deben interpretar de forma restrictiva y no permitir la transferencia frecuente, en masa y estructural de datos personales ni la transferencia de datos a gran escala, sino limitarse a los datos estrictamente necesarios. Tales transferencias deben documentarse y ponerse a disposición de la autoridad de supervisión cuando así lo solicite, a fin de supervisar la licitud de las transferencias.

(73) Las autoridades competentes de los Estados miembros están aplicando acuerdos internacionales vigentes, de carácter bilateral o multilateral, celebrados con terceros países en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial para el intercambio de información de interés que les permita desempeñar las funciones que les encomienda la ley. En principio, estos intercambios se realizan a través de las autoridades correspondientes de los terceros países en cuestión a efectos de la presente Directiva, o al menos con su cooperación, en ocasiones incluso sin que exista un acuerdo internacional bilateral o multilateral. Sin embargo, en determinados casos particulares, los procedimientos habituales que exigen contactar con la autoridad del tercer país en cuestión pueden ser ineficaces o inadecuados, en particular por no permitir efectuar la transferencia de forma oportuna, o porque dicha autoridad del tercer país no respete el Estado de Derecho o las normas y principios internacionales en materia de derechos humanos, en cuyo caso las autoridades competentes de los Estados miembros pueden decidir transferir los datos personales directamente a destinatarios establecidos en terceros países. Este caso puede darse cuando haya una necesidad urgente de transferir datos personales para

salvar la vida de una persona que esté en peligro de ser víctima de una infracción penal o para prevenir la comisión inminente de un delito, en particular, de terrorismo. Aunque dicho tipo de transferencias de datos entre autoridades competentes y destinatarios establecidos en terceros países solo debe producirse en casos concretos y específicos, la presente Directiva debe prever condiciones para la reglamentación de tales casos. Esas disposiciones no deben considerarse excepciones a ningún acuerdo internacional existente, ya sea bilateral o multilateral, en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial. Dichas normas deben aplicarse además de las demás normas de la presente Directiva, en particular las relativas a la licitud del tratamiento y las del capítulo V.

(74) Cuando los datos personales circulan a través de las fronteras, se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer sus derechos de protección de datos con el fin de protegerse contra la utilización o comunicación ilícitas de dichos datos. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades realizadas fuera de sus fronteras. Sus esfuerzos por colaborar en el ámbito transfronterizo también pueden verse obstaculizados por la insuficiencia de las facultades preventivas o correctivas o la incoherencia de los ordenamientos jurídicos. Por tanto, es necesario fomentar una cooperación más estrecha entre las autoridades de control de la protección de datos a fin de contribuir al intercambio de información con sus homólogos extranjeros.

(75) 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 personales. Las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas en aplicación de la presente Directiva y deben contribuir a su aplicación coherente en toda la Unión, con el fin de proteger a las personas físicas en relación con el tratamiento de sus datos personales. Para ello, las autoridades de control deben cooperar entre sí y con la Comisión.

(76) Los Estados miembros pueden confiar a una autoridad de control que ya haya sido creada de conformidad con el Reglamento (UE) 2016/679 la responsabilidad correspondiente a las funciones que hayan de desempeñar las autoridades nacionales de control que se creen con arreglo a lo dispuesto en la presente Directiva.

(77) Se debe autorizar a los Estados miembros a crear más de una autoridad de control con objeto de reflejar su estructura constitucional, organizativa y administrativa. Todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus funciones, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión. Cada autoridad de control debe disponer de un presupuesto anual público independiente, que podrá formar parte del presupuesto general estatal o nacional.

(78) Las autoridades de control deben estar sujetas a mecanismos de control o supervisión independientes en relación con sus gastos financieros, siempre que este control financiero no afecte a su independencia.

(79) Las condiciones generales aplicables al miembro o miembros de la autoridad de control deben establecerse en el Derecho del Estado miembro, y disponer, entre otras cosas, que dichos miembros sean nombrados por el Parlamento, o el Gobierno o el jefe de Estado del Estado miembro, a partir de una propuesta del Gobierno o de un miembro del Gobierno, o del Parlamento o su Cámara, o por un organismo independiente al que el Derecho del Estado miembro encomiende el nombramiento mediante un procedimiento transparente. Con el fin de garantizar la independencia de la autoridad de control, sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones y no deben participar, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada. Con el fin de garantizar la independencia de la autoridad de control, el personal ha de ser seleccionado por la autoridad de control, lo que podrá incluir la intervención de un organismo independiente encomendado por el Derecho del Estado miembro.

(80) Aunque la presente Directiva también se aplica a las actividades de los órganos jurisdiccionales nacionales y otras autoridades judiciales, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los órganos jurisdiccionales actúen en ejercicio de su función jurisdiccional, con el fin de garantizar la independencia de los jueces en el desempeño de sus funciones. Esta excepción debe limitarse a actividades judiciales en juicios y no debe aplicarse a otras actividades en las que puedan estar implicados los jueces, de conformidad con el Derecho del Estado miembro. Los Estados miembros pueden disponer también que la competencia de la autoridad de control no abarque el tratamiento de datos personales realizado por otras autoridades judiciales independientes en el ejercicio de su función jurisdiccional, por ejemplo la fiscalía. En todo caso, el cumplimiento de las normas de la presente Directiva por los órganos jurisdiccionales y otras autoridades judiciales independientes debe estar sujeto siempre a una supervisión independiente de conformidad con el artículo 8, apartado 3, de la Carta.

(81) Cada autoridad de control debe atender a las reclamaciones presentadas por cualquier interesado y debe investigar el asunto o transmitirlo a la autoridad de control competente. 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.

(82) Para garantizar una supervisión del cumplimiento y una ejecución eficaces, fiables y coherentes de la presente Directiva en toda la Unión con arreglo al TFUE a tenor de la interpretación del Tribunal de Justicia, las autoridades de control deben tener en cada Estado miembro las mismas funciones y los mismos poderes efectivos, incluidos los poderes de investigación, los poderes de corrección y los poderes consultivos que constituyan los medios necesarios para el desempeño de sus funciones. Sin embargo, sus competencias no deben afectar a las normas específicas previstas para los procesos penales, incluidos la investigación y el enjuiciamiento de infracciones penales, ni a la independencia del poder judicial. Sin perjuicio de las atribuciones del ministerio fiscal con arreglo al Derecho del Estado miembro, las autoridades de control deben tener también competencia para poner en conocimiento de las autoridades judiciales las infracciones de la presente Directiva y/o capacidad para litigar. Los poderes de las autoridades de control deben ejercerse de conformidad con las garantías procesales adecuadas establecidas en el Derecho de la Unión y de los Estados miembros, de forma imparcial y justa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento de la presente Directiva, teniendo en cuenta las circunstancias de cada caso concreto, respetar el derecho de todas las personas a ser oídas antes de que se adopte cualquier medida que les afecte negativamente y evitar costes superfluos y molestias excesivas para las personas afectadas. Los poderes de investigación en lo que se refiere al acceso a instalaciones deben ejercerse de conformidad con los requisitos específicos del Derecho del Estado miembro, como el de obtener una autorización judicial previa. Las decisiones jurídicamente vinculantes que se adopten deben estar sujetas a control jurisdiccional en el Estado miembro de la autoridad de control que haya adoptado la decisión.

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

(84) El Comité Europeo de Protección de Datos debe contribuir a la aplicación coherente de la presente Directiva en el conjunto de la Unión, entre otras cosas asesorando a la Comisión y fomentando la cooperación de las autoridades de control en toda la Unión.

(85) Todo interesado debe tener derecho a presentar una reclamación ante una única autoridad de control y a presentar un recurso judicial efectivo de conformidad con el artículo 47 de la Carta si considera que se vulneran sus derechos según las disposiciones adoptadas en virtud de la presente Directiva o en caso de que la autoridad de control no reaccione ante una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando su actuación sea necesaria para proteger los derechos del interesado. 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 competente 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. Para facilitar la presentación de reclamaciones, cada autoridad de control debe adoptar medidas como ofrecer un formulario de reclamaciones que pueda cumplimentarse también por vía electrónica, sin excluir otros medios de comunicación.

(86) Toda persona física o jurídica debe tener derecho a presentar un recurso judicial efectivo ante el órgano jurisdiccional nacional competente contra las decisiones de una autoridad de control que produzcan efectos jurídicos que le conciernan. Tales decisiones se refieren en particular al ejercicio de los poderes de investigación, corrección y autorización por parte de la autoridad de control o a la desestimación o rechazo de las reclamaciones. No obstante, este derecho no incluye otras medidas de las autoridades de control que no sean jurídicamente vinculantes, como los dictámenes publicados o el asesoramiento facilitado por la autoridad de control. Las acciones legales contra una autoridad de control deben ejercerse ante los órganos jurisdiccionales del Estado miembro en el que esté establecida la autoridad de control y conducirse con arreglo al Derecho del Estado miembro. Esos órganos jurisdiccionales deben ejercer la plena jurisdicción, que debe incluir la jurisdicción para examinar todas las circunstancias de hecho y de Derecho relativas al litigio en el que entiendan.

(87) Cuando el interesado considere que se conculcan sus derechos reconocidos en la presente Directiva, tendrá derecho a dar mandato a una entidad que tenga por objeto proteger los derechos e intereses de los interesados en

relación con la protección de sus datos personales y esté constituida con arreglo al Derecho del Estado miembro, para que presente, en su nombre, una reclamación ante la autoridad de control y ejerza el derecho al recurso judicial. El derecho a representación de los interesados será sin perjuicio del Derecho procesal del Estado miembro que pueda requerir una representación obligatoria de los interesados por parte de un abogado, como se define en la Directiva 77/249/CEE del Consejo ([1]), ante los tribunales nacionales.

(88) Cualquier perjuicio que pueda sufrir una persona como consecuencia de un tratamiento que infrinja disposiciones adoptadas en virtud de la presente Directiva debe ser compensado por el responsable o cualquier otra autoridad competente en virtud del Derecho del Estado miembro. El concepto de perjuicio debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia y de tal modo que refleje plenamente los objetivos de la presente Directiva. Lo anterior se entiende sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros. Las referencias a operaciones de tratamiento ilícitas o que incumplan las disposiciones adoptadas en virtud de la presente Directiva abarcan asimismo las operaciones de tratamiento que incumplan actos de ejecución adoptados en virtud de la presente Directiva. Los interesados deben recibir una compensación total y efectiva por el perjuicio sufrido.

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

(90) Con el fin de garantizar unas condiciones uniformes para la aplicación de la presente Directiva, se deben conferir competencias de ejecución a la Comisión con objeto de especificar: el nivel adecuado de protección que ofrece un tercer país, un territorio o un sector especificado en dicho tercer país o una organización internacional; el formato y los procedimientos de asistencia mutua y a las disposiciones aplicables al intercambio electrónico de información entre las autoridades de control, y entre estas y el Comité Europeo de Protección de Datos. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([2]).

(91) Debe emplearse el procedimiento de examen para la adopción de actos de ejecución sobre el nivel adecuado de protección que ofrece un tercer país, un territorio o un sector especificado en dicho tercer país o una organización internacional así como sobre el formato y los procedimientos de asistencia mutua y las disposiciones aplicables al intercambio electrónico de información entre las autoridades de control, y entre estas y el Comité Europeo de Protección de Datos, dado que dichos actos son de alcance general.

(92) 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 específico en ese tercer país, o una organización internacional que ya no garanticen un nivel de protección adecuado.

(93) Dado que los objetivos de la presente Directiva, a saber, proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales y garantizar el libre intercambio de datos personales por parte de las autoridades competentes en la Unión, no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, debido a la dimensión o los efectos de la acción, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos.

(94) No deben verse afectadas las disposiciones específicas de actos de la Unión adoptados antes de la fecha de adopción de la presente Directiva en el ámbito de la cooperación judicial en materia penal o de la cooperación policial que regulen el tratamiento de los datos personales entre los Estados miembros o el acceso de las

([1]) Directiva 77/249/CEE del Consejo, de 22 de marzo de 1977, dirigida a facilitar el ejercicio efectivo de la libre prestación de servicios por los abogados (DO L 78 de 26.3.1977, p. 17).

([2]) Reglamento (UE) n.º 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).

autoridades designadas de los Estados miembros a los sistemas de información establecidos con arreglo a lo dispuesto en los Tratados, como por ejemplo las disposiciones específicas relativas a la protección de los datos personales que se aplican en virtud de la Decisión 2008/615/JAI del Consejo ([1]), o el artículo 23 del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea ([2]). Dado que el artículo 8 de la Carta y el artículo 16 del TFUE conllevan que el derecho fundamental a la protección de los datos personales debe estar garantizado de manera coherente y homogénea en toda la Unión, la Comisión debe evaluar la situación con respecto a la relación entre la presente Directiva y los actos adoptados con anterioridad a su fecha de adopción que regulan el tratamiento de los datos personales entre los Estados miembros o el acceso de las autoridades designadas de los Estados miembros a los sistemas de información establecidos con arreglo a lo dispuesto en los Tratados, a fin de evaluar la necesidad de adaptar estas disposiciones específicas a la presente Directiva. Cuando corresponda, la Comisión debe presentar propuestas encaminadas a garantizar normas jurídicas coherentes en relación con el tratamiento de los datos personales.

(95) Con el fin de garantizar una protección amplia y coherente de los datos personales en la Unión, los acuerdos internacionales celebrados por los Estados miembros con anterioridad a la fecha de entrada en vigor de la presente Directiva y que respeten el Derecho correspondiente de la Unión aplicable antes de dicha fecha deben seguir en vigor hasta que sean modificados, sustituidos o revocados.

(96) Los Estados miembros deben poder contar con un plazo de no más de dos años desde la entrada en vigor de la presente Directiva para incorporarla a su Derecho nacional. Todo tratamiento ya iniciado en dicha fecha debe adaptarse a lo establecido en la presente Directiva en un plazo de dos años a partir de la entrada en vigor de la presente Directiva. No obstante, si dicho tratamiento cumple el Derecho de la Unión aplicable antes de la fecha de entrada en vigor de la presente Directiva, los requisitos de la presente Directiva relativos a la consulta previa a la autoridad de control no deben aplicarse a las operaciones de tratamiento ya iniciadas antes de la mencionada fecha, dado que estos requisitos, por su propia naturaleza, han cumplirse antes del tratamiento. Cuando los Estados miembros se acojan al plazo de aplicación más largo que caduca siete años después de la fecha de entrada en vigor de la presente Directiva para cumplir las obligaciones de registro aplicables a los sistemas de tratamiento automatizados establecidos con anterioridad a dicha fecha, el responsable o encargado del tratamiento deben contar con métodos eficaces de demostrar la legalidad del tratamiento de datos, de permitir el autocontrol y de asegurar la integridad y la seguridad de los datos, como las anotaciones en un registro diario.

(97) La presente Directiva se entiende sin perjuicio de las normas relativas a la lucha contra los abusos sexuales, la explotación sexual de los menores, y la pornografía infantil, tal como se establecen en la Directiva 2011/93/UE del Parlamento Europeo y del Consejo ([3]).

(98) Por consiguiente, la Decisión Marco 2008/977/JAI debe ser derogada en consecuencia.

(99) De conformidad con el artículo 6 *bis* del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al TUE y al TFUE, no son vinculantes para el Reino Unido e Irlanda las normas establecidas en la presente Directiva relativas a tratamiento de datos personales por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del capítulo 4 o el capítulo 5 del título V de la tercera parte del TFUE en la medida en que no sean vinculantes para estos Estados las normas de la Unión que regulen formas de cooperación judicial en materia penal y de cooperación policial en cuyo marco deban respetarse las disposiciones establecidas sobre la base del artículo 16 del TFUE.

(100) De conformidad con lo dispuesto en los artículos 2 y 2 *bis* del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al TUE y al TFUE, Dinamarca no queda obligada por las normas establecidas en la presente Directiva que se relacionen con el tratamiento de datos personales por parte de los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del capítulo 4 o el capítulo 5 del título V de la tercera parte del TFUE, ni está sujeta a su aplicación. Dado que la presente Directiva desarrolla el acervo de Schengen en el marco de las disposiciones del título V de la tercera parte del TFUE, de conformidad con el artículo 4 del mencionado Protocolo, Dinamarca debe decidir, en un plazo de seis meses a partir de la adopción de la presente Directiva, si lo incorpora a su legislación nacional.

(101) Por lo que se refiere a Islandia y Noruega, la presente Directiva constituye un desarrollo de las disposiciones del acervo de Schengen, como se establece en el Acuerdo celebrado por el Consejo de la Unión Europea con la República de Islandia y el Reino de Noruega sobre la asociación de estos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen ([4]).

([1]) Decisión 2008/615/JAI del Consejo, 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).

([2]) Acto del Consejo, de 29 de mayo de 2000, por el que se celebra, de conformidad con el artículo 34 del Tratado de la Unión Europea, el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea (DO C 197 de 12.7.2000, p. 1).

([3]) Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo (DO L 335 de 17.12.2011, p. 1).

([4]) DO L 176 de 10.7.1999, p. 36.

(102) Por lo que respecta a Suiza, la presente Directiva constituye un desarrollo de las disposiciones del acervo de Schengen, como se establece en el Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen ([1]).

(103) Por lo que respecta a Liechtenstein, la presente Directiva constituye un desarrollo de las disposiciones del acervo de Schengen, como se establece en el Protocolo entre la 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 ([2]).

(104) La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos en la Carta, consagrados en el TFUE, en particular el derecho al respeto de la vida privada y familiar, el derecho a la protección de los datos personales y el derecho a la tutela judicial efectiva y a un juez imparcial. Las limitaciones aplicadas a estos derechos son conformes al artículo 52, apartado 1, de la Carta ya que son necesarias para alcanzar objetivos de interés general reconocidos por la Unión o responden a la necesidad de proteger los derechos y libertades de terceros.

(105) De conformidad con la Declaración política conjunta, de 28 de septiembre de 2011, de los Estados miembros y de la Comisión sobre los documentos explicativos, en casos justificados, los Estados miembros se comprometen a adjuntar a la notificación de las medidas de transposición uno o varios documentos que expliquen la relación entre los componentes de una directiva y las partes correspondientes de las medidas nacionales de transposición. Tratándose de la presente Directiva, el legislador considera justificada la transmisión de dichos documentos.

(106) El Supervisor Europeo de Protección de Datos ha sido consultado de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001 y emitió un dictamen el 7 de marzo de 2012 ([3]).

(107) La presente Directiva no debe impedir que los Estados miembros regulen el ejercicio de los derechos de los interesados en materia de información, acceso a los datos personales, rectificación o supresión de estos y limitación de su tratamiento en el marco de un proceso penal, y las posibles restricciones de tales derechos, mediante el Derecho procesal penal nacional.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

Disposiciones generales

Artículo 1

Objeto y objetivos

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

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

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

b) garantizar que el intercambio de datos personales por parte de las autoridades competentes en el interior de la Unión, en caso de que el Derecho de la Unión o del Estado miembro exijan dicho intercambio, no quede restringido ni prohibido por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

([1]) DO L 53 de 27.2.2008, p. 52.
([2]) DO L 160 de 18.6.2011, p. 21.
([3]) DO C 192 de 30.6.2012, p. 7.

3. La presente Directiva no impedirá a los Estados miembros ofrecer mayores garantías que las que en ella se establecen para la protección de los derechos y libertades del interesado con respecto al tratamiento de datos personales por parte de las autoridades competentes.

Artículo 2

Ámbito de aplicación

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

2. La presente Directiva 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.

3. La presente Directiva 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;

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

Artículo 3

Definiciones

A efectos de la presente Directiva se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, 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, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos personales conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

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

7) «autoridad competente»:

   a) toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, o

   b) cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública;

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

9) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

10) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerará destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o del Estado miembro; el tratamiento de tales datos por las citadas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

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

12) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de la persona física de que se trate;

13) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

14) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

15) «autoridad de control»: una autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 41;

16) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

CAPÍTULO II

Principios

Artículo 4

Principios relativos al tratamiento de datos personales

1. Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera lícita y leal;

b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines;

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

d) exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados;

e) conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados;

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas.

2. Se permitirá el tratamiento de los datos personales, por el mismo responsable o por otro, para fines establecidos en el artículo 1, apartado 1, distintos de aquel para el que se recojan en la medida en que:

a) el responsable del tratamiento esté autorizado a tratar dichos datos personales para dicho fin de conformidad con el Derecho de la Unión o del Estado miembro, y

b) el tratamiento sea necesario y proporcionado para ese otro fin de conformidad con el Derecho de la Unión o del Estado miembro.

3. El tratamiento por el mismo responsable o por otro podrá incluir el archivo en el interés público, el uso científico, estadístico o histórico para los fines establecidos en el artículo 1, apartado 1, con sujeción a las salvaguardias adecuadas para los derechos y libertades de los interesados.

4. El responsable del tratamiento será responsable y capaz de demostrar el cumplimiento de lo dispuesto en los apartados 1, 2 y 3.

Artículo 5

Plazos de conservación y revisión

Los Estados miembros dispondrán que se fijen plazos apropiados para la supresión de los datos personales o para una revisión periódica de la necesidad de conservación de los datos personales. Las normas de procedimiento garantizarán el cumplimiento de dichos plazos.

Artículo 6

Distinción entre diferentes categorías de interesados

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

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

b) personas condenadas por una infracción penal;

c) víctimas de una infracción penal o personas respecto de las cuales determinados hechos den lugar a pensar que puedan ser víctimas de una infracción penal, y

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

Artículo 7

Distinción entre datos personales y verificación de la calidad de los datos personales

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

2. Los Estados miembros dispondrán que las autoridades competentes adopten todas las medidas razonables para garantizar que los datos personales que sean inexactos, incompletos o que no estén actualizados no se transmitan ni se pongan a disposición de terceros. Para ello, dicha autoridad competente, en la medida en que sea factible, controlará la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de terceros. En la medida de lo posible, en todas las transmisiones de datos personales se añadirá la información necesaria para que la autoridad competente receptora pueda valorar en qué medida los datos personales son exactos, completos y fiables y en qué medida están actualizados.

3. Si se observara que se hubieran transmitido datos personales incorrectos o se hubieran transmitido ilegalmente, el hecho deberá ponerse en conocimiento del destinatario sin dilación. En tal caso, los datos personales deberán rectificarse o suprimirse, o el tratamiento deberá limitarse de conformidad con el artículo 16.

Artículo 8

Licitud del tratamiento

1. Los Estados miembros dispondrán que el tratamiento solo sea lícito en la medida en que sea necesario para la ejecución de una tarea realizada por una autoridad competente, para los fines establecidos en el artículo 1, apartado 1, y esté basado en el Derecho de la Unión o del Estado miembro.

2. El Derecho del Estado miembro que regule el tratamiento dentro del ámbito de aplicación de la presente Directiva, deberá indicar al menos los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento.

Artículo 9

Condiciones de tratamiento específicas

1. Los datos personales recogidos por las autoridades competentes para los fines establecidos en el artículo 1, apartado 1, no serán tratados para otros fines distintos de los establecidos en el artículo 1, apartado 1 salvo que dicho tratamiento esté autorizado por el Derecho de la Unión o del Estado miembro. Cuando los datos personales sean tratados para otros fines, se aplicará el Reglamento (UE) 2016/679 a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión.

2. Cuando el Derecho del Estado miembro encomiende a las autoridades competentes el desempeño de funciones que no coincidan con los fines establecidos en el artículo 1, apartado 1, se aplicará el Reglamento (UE) 2016/679 al tratamiento con dichos fines, incluidos fines de archivo en interés público, de investigación científica e histórica o estadísticos, salvo que el tratamiento se lleve a cabo en una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión.

3. Los Estados miembros dispondrán que, cuando el Derecho de la Unión o del Estado miembro aplicable a la autoridad competente transmisora prevea condiciones específicas aplicables al tratamiento, la autoridad competente transmisora deberá informar al destinatario al que se transmitan los datos de las condiciones y la obligación de respetarlos.

4. Los Estados miembros dispondrán que la autoridad competente transmisora no aplique las condiciones del apartado 3 a los destinatarios de otros Estados miembros o a los organismos, agencias y órganos establecidos en virtud de los capítulos 4 y 5 del título V de la tercera parte del TFUE distintas de las aplicables a las transmisiones de datos similares en el Estado miembro de la autoridad competente transmisora.

Artículo 10

Tratamiento de categorías especiales de datos personales

El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física solo se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando:

a) lo autorice el Derecho de la Unión o del Estado miembro;

b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o

c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

Artículo 11

Mecanismo de decisión individual automatizado

1. Los Estados miembros dispondrán la prohibición de las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o le afecten significativamente, salvo que estén autorizadas por el Derecho de la Unión o del Estado miembro a la que esté sujeto el responsable del tratamiento y que establezca medidas adecuadas para salvaguardar los derechos y libertades del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento.

2. Las decisiones a que se refiere el apartado 1 del presente artículo no se basarán en las categorías especiales de datos personales contempladas en el artículo 10, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

3. La elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales establecidas en el artículo 10 quedará prohibida, de conformidad con el Derecho de la Unión.

CAPÍTULO III

Derechos del interesado

Artículo 12

Comunicación y modalidades del ejercicio de los derechos de los interesados

1. Los Estados miembros dispondrán que el responsable tome medidas razonables para facilitar al interesado toda información contemplada en el artículo 13, así como cualquier comunicación contemplada en los artículos 11, 14 a 18 y 31 relativa al tratamiento, en forma concisa, inteligible y de fácil acceso, con un lenguaje claro y sencillo. La información será facilitada por cualquier medio adecuado, inclusive por medios electrónicos. Como norma general, el responsable facilitará la información por medio idéntico al utilizado para la solicitud.

2. Los Estados miembros dispondrán que el responsable del tratamiento facilite el ejercicio de los derechos del interesado en virtud de los artículos 11 y 14 a 18.

3. Los Estados miembros dispondrán que el responsable del tratamiento informe por escrito al interesado, sin dilación indebida, sobre el curso dado a su solicitud.

4. Los Estados miembros dispondrán que la información facilitada con arreglo al artículo 13 y cualquier comunicación efectuada y acción realizada en virtud de los artículos 11, 14 a 18 y 31 serán a título gratuito. Cuando las solicitudes de un interesado sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable, teniendo en cuenta los costes administrativos afrontados para facilitar la información o la comunicación o realizar la acción solicitada, o

b) negarse a actuar según lo solicitado.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

5. Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que curse la solicitud a que se refieren los artículos 14 y 16, podrá solicitar que se facilite la información complementaria necesaria para confirmar la identidad del interesado.

Artículo 13

Información que debe ponerse a disposición del interesado o que se le debe proporcionar

1. Los Estados miembros dispondrán que el responsable del tratamiento de los datos ponga a disposición del interesado al menos la siguiente información:

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

b) en su caso, los datos de contacto del delegado de protección de datos;

c) los fines del tratamiento a que se destinen los datos personales;

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

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

2. Además de la información indicada en el apartado 1, los Estados miembros dispondrán por ley que el responsable del tratamiento de los datos proporcione al interesado, en casos concretos, la siguiente información adicional, a fin de permitir el ejercicio de sus derechos:

a) la base jurídica del tratamiento;

b) el plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo;

c) cuando corresponda, las categorías de destinatarios de los datos personales, en particular en terceros países u organizaciones internacionales;

d) cuando sea necesario, más información, en particular cuando los datos personales se hayan recogido sin conocimiento del interesado.

3. Los Estados miembros podrán adoptar medidas legislativas por las que se retrase, limite u omita la puesta a disposición del interesado de la información en virtud del apartado 2 siempre y cuando dicha medida constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para:

a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales;

b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales;

c) proteger la seguridad pública;

d) proteger la seguridad nacional;

e) proteger los derechos y libertades de otras personas.

4. Los Estados miembros podrán adoptar medidas legislativas para determinar las categorías de tratamiento que pueden incluirse, total o parcialmente, en cualquiera de las letras del apartado 3.

Artículo 14

Derecho de acceso del interesado a los datos personales

Con sujeción a lo dispuesto en el artículo 15, los Estados miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en caso de que se confirme el tratamiento, acceso a dichos datos personales y la siguiente información:

a) los fines y la base jurídica del tratamiento;

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

c) los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales, en particular los destinatarios establecidos en terceros países o las organizaciones internacionales;

d) cuando sea posible, el plazo contemplado durante el cual se conservarán los datos personales o, de no ser posible, los criterios utilizados para determinar dicho plazo;

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

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.

Artículo 15

Limitaciones al derecho de acceso

1. Los Estados miembros podrán adoptar medidas legislativas por las que se restrinja, total o parcialmente, el derecho de acceso del interesado siempre y cuando dicha restricción parcial o completa constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para:

a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales;

b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales;

c) proteger la seguridad pública;

d) proteger la seguridad nacional;

e) proteger los derechos y libertades de otras personas.

2. Los Estados miembros podrán adoptar medidas legislativas para determinar las categorías de tratamiento que pueden acogerse, total o parcialmente, a las exenciones del apartado 1.

3. En los casos contemplados en los apartados 1 y 2, los Estados miembros dispondrán que el responsable del tratamiento informe por escrito al interesado, sin dilación indebida, de cualquier denegación o limitación de acceso, y de las razones de la denegación o de la restricción. Esta información podrá omitirse cuando el suministro de dicha información pueda comprometer uno de los fines contemplados en el apartado 1. Los Estados miembros dispondrán que el responsable del tratamiento informe al interesado de las posibilidades de presentar una reclamación ante la autoridad de control y de interponer un recurso judicial.

4. Los Estados miembros velarán por que el responsable del tratamiento documente los fundamentos de hecho o de Derecho en los que se sustente la decisión. Dicha información se pondrá a disposición de las autoridades de control.

Artículo 16

Derecho de rectificación o supresión de datos personales y limitación de su tratamiento

1. Los Estados miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento sin dilación indebida la rectificación de los datos personales que le conciernan cuando tales datos resulten inexactos. Teniendo en cuenta la finalidad del tratamiento, los Estados miembros dispondrán que el interesado tenga derecho a que se completen los datos personales cuando estos resulten incompletos, en particular mediante una declaración suplementaria.

2. Los Estados miembros exigirán al responsable del tratamiento suprimir los datos personales sin dilación indebida y dispondrán el derecho del interesado a obtener del responsable del tratamiento la supresión de los datos personales que le conciernan sin dilación indebida cuando el tratamiento infrinja los artículos 4, 8 o 10, o cuando los datos personales deban ser suprimidos en virtud de una obligación legal a la que esté sujeto el responsable del tratamiento.

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

a) el interesado ponga en duda la exactitud de los datos personales y no pueda determinarse la exactitud o inexactitud, o

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

Cuando el tratamiento esté limitado en virtud del párrafo primero, letra a), el responsable del tratamiento informará al interesado antes de levantar la limitación del tratamiento.

4. Los Estados miembros dispondrán que el responsable del tratamiento informe al interesado por escrito de cualquier denegación de rectificación o supresión de los datos personales, o de limitación de su tratamiento, y de las razones de la denegación. Los Estados miembros podrán adoptar medidas legislativas por las que se restrinja, total o parcialmente, la obligación de proporcionar tal información, en siempre y cuando dicha limitación del tratamiento constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para:

a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales;

b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales;

c) proteger la seguridad pública;

d) proteger la seguridad nacional;

e) proteger los derechos y libertades de otras personas.

Los Estados miembros dispondrán que el responsable del tratamiento informe al interesado de las posibilidades de presentar una reclamación ante la autoridad de control y de interponer un recurso judicial.

5. Los Estados miembros dispondrán que el responsable del tratamiento comunique la rectificación de los datos personales inexactos a la autoridad competente de la que procedan los datos personales inexactos.

6. Los Estados miembros dispondrán que, cuando los datos personales hayan sido rectificados o suprimidos o el tratamiento haya sido limitado en virtud de los apartados 1, 2 y 3, el responsable del tratamiento lo notifique a los destinatarios y que estos rectifiquen o supriman los datos personales que estén bajo su responsabilidad, o limiten su tratamiento.

Artículo 17

Ejercicio de los derechos del interesado y comprobación por la autoridad de control

1. En los casos contemplados en el artículo 13, apartado 3, en el artículo 15, apartado 3, y en el artículo 16, apartado 4, los Estados miembros adoptarán medidas por las que se disponga que los derechos del interesado también puedan ejercerse a través de la autoridad de control competente.

2. Los Estados miembros dispondrán que el responsable del tratamiento informe al interesado de la posibilidad de ejercer sus derechos a través de la autoridad de control con arreglo a lo dispuesto en el apartado 1.

3. Cuando se ejerza el derecho contemplado en el apartado 1, la autoridad de control informará, al menos, al interesado de que se han efectuado todas las comprobaciones necesarias o la revisión correspondiente. La autoridad de control informará también al interesado de su derecho a la tutela judicial.

Artículo 18

Derechos del interesado en las investigaciones y los procesos penales

Los Estados miembros podrán disponer que el ejercicio de los derechos a los que se hace referencia en los artículos 13, 14 y 16 se lleve a cabo de conformidad con el Derecho del Estado miembro cuando los datos personales figuren en una resolución judicial o en un registro o expediente tramitado en el curso de investigaciones y procesos penales.

CAPÍTULO IV

Responsable del tratamiento y encargado del tratamiento

Sección 1

Obligaciones generales

Artículo 19

Obligaciones del responsable del tratamiento

1. Los Estados miembros dispondrán que el responsable del tratamiento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, aplique las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento se lleva a cabo de conformidad con la presente Directiva. Tales medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

Artículo 20

Protección de datos desde el diseño y por defecto

1. Los Estados miembros dispondrán que el responsable del tratamiento, teniendo en cuenta el estado de la técnica y el coste de la aplicación, y la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas planteados por el tratamiento, aplique, tanto en el momento de determinar los medios para el tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas, como por ejemplo la seudonimización, concebidas para aplicar los principios de protección de datos, como por ejemplo la minimización de datos, de forma efectiva y para integrar las garantías necesarias en el tratamiento, de tal manera que este cumpla los requisitos de la presente Directiva y se protejan los derechos de los interesados.

2. Los Estados miembros dispondrán que el responsable del tratamiento aplique las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Dicha obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su período de conservación y a su accesibilidad. En concreto, tales medidas garantizarán que, por defecto, los datos personales no sean accesibles, sin intervención de la persona, a un número indeterminado de personas físicas.

Artículo 21

Corresponsables del tratamiento

1. Los Estados miembros dispondrán que, cuando dos o más responsables del tratamiento determinen conjuntamente los objetivos y los medios de tratamiento, sean considerados corresponsables del tratamiento. Determinarán, de modo transparente y de mutuo acuerdo, cuáles serán sus responsabilidades respectivas en el cumplimiento de la presente Directiva, en particular por lo que se refiere al ejercicio de los derechos del interesado y a sus respectivas obligaciones en el suministro de la información contemplada en el artículo 13, salvo y en la medida en que las responsabilidades respectivas de los responsables se rijan por el Derecho de la Unión o del Estado miembro a que estén sujetos los responsables del tratamiento. El citado acuerdo designará el punto de contacto para los interesados. Los Estados miembros podrán designar cuál de los corresponsables puede actuar como punto único de contacto para el interesado por lo que respecta al ejercicio de sus derechos.

2. Independientemente de los términos del acuerdo a que hace referencia el apartado 1, los Estados miembros podrán disponer que el interesado pueda ejercer los derechos que le reconocen las disposiciones adoptadas con arreglo a la presente Directiva con respecto a cada uno de los responsables y frente a ellos.

Artículo 22

Encargado del tratamiento

1. Los Estados miembros dispondrán que, cuando una operación de tratamiento vaya a ser llevada a cabo por cuenta de un responsable del tratamiento, este recurra únicamente a encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la presente Directiva y garantice la protección de los derechos del interesado.

2. Los Estados miembros dispondrán que el encargado del tratamiento no recurra a otro encargado sin la autorización previa por escrito, específica o general, del responsable del tratamiento. En el caso de la autorización por escrito general, el encargado informará siempre al responsable de cualquier cambio previsto referido a la adición o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. Los Estados miembros dispondrán que el tratamiento por un encargado se rija por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de un Estado miembro que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, su naturaleza y finalidad, el tipo de datos personales y categorías de interesados y las obligaciones y derechos del responsable. Dicho contrato u otro acto jurídico estipulará, en particular, que el encargado del tratamiento:

a) actúe únicamente siguiendo las instrucciones del responsable del tratamiento;

b) garantice que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación profesional de confidencialidad;

c) asista al responsable del tratamiento por cualquier medio adecuado para garantizar el cumplimiento de las disposiciones sobre los derechos del interesado;

d) a elección del responsable del tratamiento, suprima o devuelva todos los datos personales al responsable del tratamiento una vez finalice la prestación de los servicios de tratamiento, y suprima las copias existentes a menos que el Derecho de la Unión o del Estado miembro requieran la conservación de los datos personales;

e) ponga a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento del presente artículo;

f) respete las condiciones indicadas en los apartados 2 y 3 para contratar a otro encargado del tratamiento.

4. El contrato u otro acto jurídico a que se refiere el apartado 3 se establecerá por escrito, inclusive en formato electrónico.

5. Si un encargado del tratamiento, infringiendo la presente Directiva, determinase los fines y medios de dicho tratamiento, será considerado responsable con respecto a ese tratamiento.

Artículo 23

Tratamiento bajo la autoridad del responsable o del encargado del tratamiento

Los Estados miembros dispondrán que el encargado del tratamiento, así como cualquier persona que actúe bajo la autoridad del responsable o del encargado del tratamiento y tenga acceso a datos personales, solo pueda 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 24

Registros de las actividades de tratamiento

1. Los Estados miembros dispondrán que cada responsable conserve un registro de todas las categorías de actividades de tratamiento de datos personales efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información siguiente:

a) el nombre y los datos de contacto del responsable del tratamiento y, en su caso, del corresponsable y del delegado de protección de datos;

b) los fines del tratamiento;

c) las categorías de destinatarios a quienes se hayan comunicado o vayan a comunicarse los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

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

e) en su caso, el recurso a la elaboración de perfiles;

f) en su caso, las categorías de transferencias de datos personales a un tercer país o a una organización internacional;

g) una indicación de la base jurídica del tratamiento, incluidas las transferencias, de que van a ser objeto los datos personales;

h) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos personales;

i) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 29, apartado 1.

2. Los Estados miembros dispondrán que cada encargado del tratamiento lleve un registro de todas las categorías de actividades de tratamiento de datos personales efectuadas en nombre de un responsable, el cual contendrá:

a) el nombre y los datos de contacto del encargado o encargados del tratamiento, de cada responsable del tratamiento en cuyo nombre actúe el encargado y, si ha lugar, el delegado de protección de datos;

b) las categorías de tratamientos efectuados en nombre de cada responsable;

c) en su caso, las transferencias de datos personales a un tercer país o a una organización internacional, incluida, cuando el responsable del tratamiento así lo ordene explícitamente, la identificación de dicho tercer país o de dicha organización internacional;

d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 29, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 se establecerán por escrito, inclusive en formato electrónico.

El responsable y el encargado del tratamiento harán que los registros estén disponibles para la autoridad de control a solicitud de esta.

Artículo 25

Registro de operaciones

1. Los Estados miembros velarán por que se conserven registros de, al menos, las operaciones de tratamiento en sistemas de tratamiento automatizados siguientes: recogida, alteración, consulta, comunicación incluidas las transferencias, combinación o supresión. Los registros de consulta y comunicación harán posible determinar la justificación, la fecha y la hora de tales operaciones y, en la medida de lo posible, el nombre de la persona que consultó o comunicó datos personales, así como la identidad de los destinatarios de dichos datos personales.

2. Dichos registros se utilizarán únicamente a efectos de verificar la legalidad del tratamiento, autocontrol, garantizar la integridad y la seguridad de los datos personales y en el ámbito de los procesos penales.

3. El responsable y el encargado del tratamiento pondrán los registros de operaciones a disposición de la autoridad de control a solicitud de esta.

Artículo 26

Cooperación con la autoridad de control

Los Estados miembros dispondrán que el responsable y el encargado del tratamiento cooperen con la autoridad de control, cuando esta lo solicite, en el desempeño de sus funciones.

Artículo 27

Evaluación de impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas físicas, los Estados miembros dispondrán que el responsable del tratamiento lleve a cabo, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.

2. La evaluación mencionada en el apartado 1 incluirá, 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 estos riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar la conformidad con la presente Directiva, teniendo en cuenta los derechos e intereses legítimos de los interesados y las demás personas afectadas.

Artículo 28

Consulta previa a la autoridad de control

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

a) la evaluación del impacto en la protección de los datos que prevé el artículo 27 indique que el tratamiento entrañaría un alto riesgo a falta de medidas adoptadas por el responsable a fin de mitigar el riesgo, o

b) el tipo de tratamiento, en particular cuando se usen tecnologías, mecanismos o procedimientos nuevos, constituya un alto riesgo para los derechos y libertades de los interesados.

2. Los Estados miembros dispondrán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que deba ser adoptada por un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que guarde relación con el tratamiento.

3. Los Estados miembros dispondrán que la autoridad de control pueda establecer una lista de las operaciones de tratamiento que están sujetas a consulta previa con arreglo a lo dispuesto en el apartado 1.

4. Los Estados miembros dispondrán que el responsable del tratamiento facilite a la autoridad de control la evaluación de impacto relativa a la protección de datos contemplada en el artículo 27 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.

5. Los Estados miembros dispondrán que, cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 del presente artículo podría infringir lo dispuesto en la presente Directiva, en particular cuando el responsable del tratamiento no haya identificado o mitigado suficientemente el riesgo, dicha autoridad de control deberá, en un plazo de seis semanas desde la solicitud de la consulta, asesorar por escrito al responsable del tratamiento y, en su caso, al encargado del tratamiento, y podrá ejercer cualquiera de sus poderes mencionados en el artículo 47. Este plazo podrá prorrogarse un mes, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado, de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, junto con los motivos de la dilación.

Sección 2

Seguridad de los datos personales

Artículo 29

Seguridad del tratamiento

1. Los Estados miembros dispondrán que el responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, sobre todo en lo que se refiere al tratamiento de las categorías especiales de datos personales previstas en el artículo 10.

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

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

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

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

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

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

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

g) garantizar que pueda verificarse y constatarse *a posteriori* qué datos personales se han introducido en los sistemas de tratamiento automatizado y en qué momento y por qué persona han sido introducidos (control de la introducción);

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

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

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

Artículo 30

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

1. Los Estados miembros dispondrán que, en caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control sin dilación indebida, y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que la violación de la seguridad de los datos personales constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no se hace en el plazo de 72 horas, deberá ir acompañada de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

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

a) describir la naturaleza de la violación de la seguridad de los datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre 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) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar sus posibles efectos negativos.

4. Si no fuera posible, o en la medida en que no sea posible, facilitar la información simultáneamente, se podrá facilitar la información por etapas sin dilación indebida.

5. Los Estados miembros dispondrán que el responsable del tratamiento documente cualquier violación de la seguridad de los datos personales a que se hace referencia en el apartado 1, incluidos los hechos relativos a dicha violación, sus efectos y las medidas correctivas adoptadas. Dicha documentación deberá permitir a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

6. Los Estados miembros dispondrán que cuando la violación de la seguridad de los datos personales tenga que ver con datos que hayan sido transmitidos por el responsable del tratamiento o al responsable del tratamiento de otro Estado miembro, la información a que se refiere el apartado 3 se comunique al responsable del tratamiento de este Estado miembro sin dilación indebida.

Artículo 31

Comunicación de una violación de la seguridad de los datos personales al interesado

1. Los Estados miembros dispondrán que, cuando sea probable que la violación de la seguridad de los datos personales vaya a dar lugar a un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento comunique al interesado, sin dilación indebida, la violación de la seguridad de los datos personales.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá con un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá, al menos, la información y las medidas a que se refiere el artículo 30, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y dichas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no sea probable que se materialice el alto riesgo para los derechos y libertades del interesado a que hace referencia el apartado 1;

c) suponga un esfuerzo desproporcionado. En este supuesto, se optará a cambio por una comunicación pública o una medida semejante mediante la cual se informe a los interesados de manera igualmente efectiva.

4. Cuando el responsable del tratamiento no haya comunicado todavía al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación suponga un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones que cita el apartado 3.

5. La comunicación al interesado a que se hace referencia en el apartado 1 del presente artículo podrá aplazarse, limitarse u omitirse con sujeción a las condiciones y por los motivos que se contemplan en el artículo 13, apartado 3.

Sección 3

Delegado de protección de datos

Artículo 32

Designación del delegado de protección de datos

1. Los Estados miembros dispondrán que el responsable del tratamiento designe un delegado de protección de datos. Los Estados miembros podrán eximir de esa obligación a los tribunales y demás autoridades judiciales independientes cuando actúen en ejercicio de sus competencias judiciales.

2. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos, y a su capacidad para desempeñar las funciones contempladas en el artículo 34.

3. Podrá designarse a un único delegado de protección de datos para varias autoridades competentes teniendo en cuenta la estructura organizativa y tamaño de estas.

4. Los Estados miembros dispondrán que el responsable del tratamiento publique los datos de contacto del delegado de protección de datos y los comunique a la autoridad de control.

Artículo 33

Posición del delegado de protección de datos

1. Los Estados miembros dispondrán que el responsable del tratamiento vele por que el delegado de protección de datos participe adecuada y oportunamente en todas las cuestiones relativas a la protección de datos personales.

2. El responsable del tratamiento respaldará al delegado de protección de datos en el desempeño de las funciones contempladas en el artículo 34 facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, así como para mantener sus conocimientos especializados.

Artículo 34

Funciones del delegado de protección de datos

Los Estados miembros dispondrán que el responsable del tratamiento encomiende al delegado de protección de datos, como mínimo, las siguientes funciones:

a) informar y asesorar al responsable del tratamiento y a los empleados que se ocupen del mismo de las obligaciones que les incumben en virtud de la presente Directiva y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en la presente Directiva, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable del tratamiento en materia de protección de datos personales, incluidas la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le pida acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización de conformidad con el artículo 27;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para las cuestiones relacionadas con el tratamiento, incluida la consulta previa a que hace referencia el artículo 28, y realizar consultas, en su caso, sobre cualquier otro asunto.

CAPÍTULO V

Transferencias de datos personales a terceros países u organizaciones internacionales

Artículo 35

Principios generales de las transferencias de datos personales

1. Los Estados miembros dispondrán que cualquier transferencia de datos personales por las autoridades competentes en curso de tratamiento o que vayan a tratarse después de su transferencia a un tercer país o a una organización internacional, incluidas las transferencias ulteriores a otro tercer país u otra organización internacional, pueda realizarse en cumplimiento de las disposiciones nacionales adoptadas a tenor de otras disposiciones de la presente Directiva, solamente cuando se hayan cumplido las condiciones previstas en el presente capítulo, esto es:

a) la transferencia sea necesaria a los fines establecidos en el artículo 1, apartado 1;

b) los datos personales se transfieran a un responsable del tratamiento de un tercer país u organización internacional que sea una autoridad pública competente a los fines mencionados en el artículo 1, apartado 1;

c) en caso de que los datos personales se transmitan o procedan de otro Estado miembro, dicho Estado miembro haya dado su autorización previa para la transferencia de conformidad con el Derecho nacional:

d) la Comisión haya adoptado una decisión de adecuación con arreglo al artículo 36 o, a falta de dicha decisión, cuando las garantías apropiadas se obtengan o existan de conformidad con el artículo 37 o, a falta de una decisión de adecuación en virtud del artículo 36 y de las garantías apropiadas de conformidad con el artículo 37, se apliquen excepciones para situaciones específicas de conformidad con el artículo 38, y

e) cuando se trate de una transferencia ulterior a otro tercer país u organización internacional, la autoridad competente que haya efectuado la transferencia inicial u otra autoridad competente del mismo Estado miembro autorice la transferencia ulterior, una vez considerados debidamente todos los factores pertinentes, entre estos la gravedad de la infracción penal, la finalidad para la que se transfirieron inicialmente los datos personales y el nivel de protección de los datos personales existente en el tercer país u organización internacional a los que se transfieran ulteriormente los datos personales.

2. Los Estados miembros dispondrán que las transferencias sin autorización previa de otro Estado miembro según lo dispuesto en el apartado 1, letra c), solo se permitan si la transferencia de datos personales es necesaria a fin de prevenir una amenaza inmediata y grave para la seguridad pública de un Estado miembro, o de un tercer país, o para los intereses fundamentales de un Estado miembro, y la autorización previa no puede conseguirse a su debido tiempo. Se informará sin dilación a la autoridad responsable de conceder la autorización previa.

3. Todas las disposiciones del presente capítulo se aplicarán a fin de garantizar que no se menoscabe el nivel de protección de las personas físicas que garantiza la presente Directiva.

Artículo 36

Transferencias basadas en una decisión de adecuación

1. Los Estados miembros dispondrán que pueda realizarse una transferencia de datos personales a un tercer país o una organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los elementos siguientes:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluidas la seguridad pública, la defensa, la seguridad nacional, el Derecho penal y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de los datos, las normas profesionales y las medidas de seguridad, incluidas las normas para las transferencias ulteriores de datos personales a otro tercer país u organización internacional que se apliquen en el tercer país o en la organización internacional en cuestión, la jurisprudencia, así como los derechos del interesado efectivos y exigibles y un derecho de recurso administrativo y judicial efectivo de los interesados cuyos datos personales son transferidos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las que esté sujeta una organización internacional, con la responsabilidad de garantizar y ejecutar el cumplimiento de las normas en materia de protección de datos, incluidos los poderes ejecutivos adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos y de cooperar con las autoridades de control de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país o la organización internacional correspondiente, u otras obligaciones que deriven de convenios o instrumentos jurídicamente vinculantes o de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución contendrá un mecanismo para su revisión periódica, como mínimo cada cuatro años, que tendrá en cuenta todos los acontecimientos que sean de interés en el tercer país u organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial y, cuando proceda, determinará cuál es la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 58, apartado 2.

4. La Comisión supervisará de forma permanente los acontecimientos en los terceros países y organizaciones internacionales que pudiesen afectar al funcionamiento de las decisiones adoptadas en virtud del apartado 3.

5. Cuando así lo revele la información disponible, en particular a raíz de la revisión prevista en el apartado 3 del presente artículo, la Comisión podrá decidir que un tercer país, o uno o más sectores específicos en ese tercer país, o una organización internacional han dejado de garantizar un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo y podrá, en caso necesario, derogar, modificar o suspender la decisión a que se refiere el apartado 3 del presente artículo, mediante actos de ejecución, sin efecto retroactivo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen contemplado en el artículo 58, apartado 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento contemplado en el artículo 58, apartado 3.

6. La Comisión entablará consultas con el tercer país o la organización internacional con vistas a poner remedio a la situación que haya originado la decisión adoptada de conformidad con lo dispuesto en el apartado 5.

7. Los Estados miembros dispondrán que toda decisión de conformidad con lo dispuesto en el apartado 5 del presente artículo se entienda sin perjuicio de las transferencias de datos personales al tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de lo dispuesto en los artículos 37 y 38.

8. La Comisión publicará en el *Diario Oficial de la Unión Europea* y en su página web una lista de los terceros países, territorios y sectores específicos en un tercer país, y de las organizaciones internacionales para los que haya decidido que sigue o no garantizado un nivel de protección adecuado.

Artículo 37

Transferencias mediante garantías apropiadas

1. En ausencia de una decisión con arreglo a lo dispuesto en el artículo 36, apartado 3, los Estados miembros dispondrán que pueda producirse una transferencia de datos personales a un tercer país o una organización internacional cuando:

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

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

2. El responsable del tratamiento informará a la autoridad de control acerca de las categorías de transferencias a tenor del apartado 1, letra b).

3. Cuando las transferencias se basen en lo dispuesto en el apartado 1, letra b), deberán documentarse y la documentación se pondrá a disposición de la autoridad de control previa solicitud, con inclusión de la fecha y la hora de la transferencia, información sobre la autoridad competente destinataria, la justificación de la transferencia y los datos personales transferidos.

Artículo 38

Excepciones para situaciones específicas

1. En ausencia de una decisión de adecuación de conformidad con el artículo 36, o de garantías apropiadas de conformidad con el artículo 37, los Estados miembros dispondrán que pueda procederse a una transferencia o categoría de transferencias de datos personales a un tercer país o una organización internacional únicamente cuando la transferencia sea necesaria:

a) para proteger los intereses vitales del interesado o de otra persona;

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

c) para prevenir una amenaza grave e inmediata para la seguridad pública de un Estado miembro o de un tercer país;

d) en casos individuales a efectos del artículo 1, apartado 1, o

e) en un caso individual para el establecimiento, el ejercicio o la defensa de acciones legales en relación con los fines expuestos en el artículo 1, apartado 1.

2. Los datos personales no se transferirán si la autoridad competente de la transferencia determina que los derechos y libertades fundamentales del interesado en cuestión prevalecen sobre el interés público en la transferencia establecido en las letras d) y e) del apartado 1.

3. Cuando las transferencias se basen en lo dispuesto en el apartado 1, deberán documentarse y la documentación se pondrá a disposición, previa solicitud, de la autoridad de control, con inclusión de la fecha y la hora de la transferencia, información sobre la autoridad competente destinataria, la justificación de la transferencia y los datos personales transferidos.

Artículo 39

Transferencias de datos personales a destinatarios establecidos en terceros países

1. No obstante lo dispuesto en el artículo 35, apartado 1, letra b), y sin perjuicio de todo acuerdo internacional mencionado en el apartado 2 del presente artículo, el Derecho de la Unión o del Estado miembro podrá disponer que las autoridades competentes que cita el artículo 3, punto 7, letra a), en casos particulares y específicos, transfieran datos personales directamente a destinatarios establecidos en terceros países únicamente si se cumplen las demás disposiciones de la presente Directiva y se satisfacen todas las condiciones siguientes:

a) la transferencia sea estrictamente necesaria para la realización de una función de la autoridad competente de la transferencia según dispone el Derecho de la Unión o del Estado miembro a los fines expuestos en el artículo 1, apartado 1;

b) la autoridad competente de la transferencia determine que ninguno de los derechos y libertades fundamentales del interesado en cuestión son superiores al interés público que precise de la transferencia de que se trate;

c) la autoridad competente de la transferencia considere que la transferencia a una autoridad competente del tercer país a los fines que contempla el artículo 1, apartado 1, resulta ineficaz o inadecuada, sobre todo porque no pueda efectuarse dentro de plazo;

d) se informe sin dilación indebida a la autoridad competente del tercer país a los fines que contempla el artículo 1, apartado 1, a menos que ello sea ineficaz o inadecuado;

e) la autoridad competente de la transferencia informe al destinatario de la finalidad o finalidades específicas por las que los datos personales vayan a tratarse por esta última solamente cuando dicho tratamiento sea necesario.

2. Por acuerdo internacional mencionado en el apartado 1 se entenderá todo acuerdo internacional bilateral o multinacional en vigor entre los Estados miembros y terceros países en el ámbito de la cooperación judicial en asuntos penales y de la cooperación policial.

3. La autoridad competente de la transferencia informará a la autoridad de control acerca de las transferencias efectuadas a tenor del presente artículo.

4. Cuando las transferencias se basen en el apartado 1, deberán documentarse.

Artículo 40

Cooperación internacional en el ámbito de la protección de datos personales

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

a) crear mecanismos de cooperación internacional que faciliten la aplicación efectiva 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 correspondientes partes interesadas 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 prácticas en materia de protección de datos personales, inclusive en los conflictos jurisdiccionales con terceros países.

CAPÍTULO VI

Autoridades de control independientes

Sección 1

Independencia

Artículo 41

Autoridad de control

1. Cada Estado miembro dispondrá que sea responsabilidad de una o varias autoridades públicas independientes supervisar la aplicación de la presente Directiva, 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 (en lo sucesivo, «autoridad de control»).

2. Cada autoridad de control contribuirá a la aplicación coherente de la presente Directiva en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión de conformidad con el capítulo VII.

3. Los Estados miembros podrán disponer que una autoridad de control creada en virtud del Reglamento (UE) 2016/679 pueda ser la autoridad de control mencionada en la presente Directiva y asuma la responsabilidad de las funciones de la autoridad de control que vayan a crearse de conformidad con el apartado 1 del presente artículo.

4. Cuando en un Estado miembro estén establecidas varias autoridades de control, dicho Estado miembro designará la autoridad de control que vaya a representar a dichas autoridades en el Comité Europeo de Protección de Datos a que se refiere el artículo 51.

Artículo 42

Independencia

1. Los Estados miembros velarán por que cada autoridad de control actúe con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con la presente Directiva.

2. Los Estados miembros dispondrán que el miembro o miembros de sus autoridades de control, en el cumplimiento de sus funciones y el ejercicio de sus poderes de conformidad con la presente Directiva, se mantengan libres de toda influencia exterior, tanto directa como indirecta, y no soliciten ni acepten instrucciones de nadie.

3. Los miembros de las autoridades de control de los Estados miembros 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. Los Estados miembros velarán por que cada autoridad de control disponga de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité Europeo de Protección de Datos.

5. Los Estados miembros velarán por que cada autoridad de control disponga de su propio personal, designado por ella, que estará sujeto a la dirección exclusiva del miembro o miembros de la autoridad de control de que se trate.

6. Los Estados miembros velarán por que cada autoridad de control esté sujeta a control financiero, sin que ello afecte a su independencia y disponga de un presupuesto separado, público y anual, que podrá formar parte del presupuesto general estatal o nacional.

Artículo 43

Condiciones generales aplicables a los miembros de la autoridad de control

1. Los Estados miembros dispondrán que cada miembro de su autoridad de control sea nombrado mediante un procedimiento transparente por:

— su Parlamento,

— su Gobierno,

— su Jefe de Estado, o

— un organismo independiente encargado del nombramiento en virtud del Derecho del Estado miembro.

2. Cada miembro poseerá las cualificaciones, la experiencia y las aptitudes, especialmente en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus obligaciones y el ejercicio de sus poderes.

3. Las obligaciones de los miembros terminarán cuando expire su mandato o en caso de dimisión o jubilación obligatoria de conformidad con el Derecho del Estado miembro de que se trate.

4. Un miembro solamente podrá ser destituido en caso de conducta irregular grave o si deja de reunir las condiciones exigidas para el cumplimiento de sus obligaciones.

Artículo 44

Normas relativas al establecimiento de la autoridad de control

1. Cada Estado miembro dispondrá por ley todos los elementos indicados a continuación:

a) el establecimiento de cada autoridad de control;

b) las cualificaciones y condiciones de idoneidad requeridas para ser nombrado miembro de cada autoridad de control;

c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;

d) la duración del mandato del miembro o miembros de cada autoridad de control, que no será inferior a cuatro años, salvo los primeros nombramientos después del 6 de mayo de 2016, 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 espaciados;

e) el carácter renovable o no del mandato del miembro o miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;

f) las condiciones por las que se rigen las obligaciones del miembro o miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo y las normas que rigen el cese en el empleo.

2. El miembro o miembros y el personal de cada autoridad de control estarán sujetos, conforme al Derecho de la Unión o del Estado miembro, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, este deber de secreto profesional se aplicará en particular a la información que faciliten las personas físicas sobre infracciones de la presente Directiva.

Sección 2

Competencia, funciones y poderes

Artículo 45

Competencia

1. Los Estados miembros dispondrán que cada autoridad de control sea competente para desempeñar las funciones asignadas y ejercer los poderes que se le confieran de conformidad con la presente Directiva en el territorio de su Estado miembro.

2. Los Estados miembros dispondrán que cada autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por los órganos jurisdiccionales en el ejercicio de su función judicial. Los Estados miembros podrán disponer que su autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por otras autoridades judiciales independientes en el ejercicio de su función judicial.

Artículo 46

Funciones

1. Los Estados miembros dispondrán que cada autoridad de control esté facultada en su territorio para:

a) supervisar y hacer cumplir la aplicación de las disposiciones adoptadas con arreglo a la presente Directiva y sus medidas de ejecución;

b) promover la sensibilización y la comprensión del público acerca de los riesgos, normas, garantías y derechos relativos al tratamiento;

c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos, acerca de las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;

d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud de la presente Directiva;

e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud de la presente Directiva y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;

f) tratar las reclamaciones presentadas por un interesado o un organismo, organización o asociación de conformidad con el artículo 55, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

g) controlar la licitud del tratamiento con arreglo a lo dispuesto en el artículo 17 e informar al interesado en un plazo razonable sobre el resultado del control, de conformidad con el artículo 17, apartado 3, o sobre los motivos por los que no se ha llevado a cabo;

h) cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de velar por la coherencia en la aplicación y ejecución de la presente Directiva;

i) llevar a cabo investigaciones sobre la aplicación de la presente Directiva, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;

j) hacer un seguimiento de acontecimientos que sean 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;

k) prestar asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 28, y

l) contribuir a las actividades del Comité Europeo de Protección de Datos.

2. Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como el suministro de un formulario de reclamaciones que pueda también cumplimentarse por vía electrónica, sin excluir otros medios de comunicación.

3. El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá cobrar una tasa razonable basada en los costes administrativos, o negarse a actuar respecto de la solicitud. La carga de la demostración del carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Artículo 47

Poderes

1. Cada Estado miembro dispondrá por ley que su autoridad de control tenga poderes de investigación efectivos. Dichos poderes incluirán al menos el poder de obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales que se están tratando y a toda la información necesaria para el desempeño de sus funciones.

2. Cada Estado miembro dispondrá por ley que su autoridad de control tenga poderes correctivos efectivos como, por ejemplo:

a) formular a todo responsable o encargado del tratamiento una advertencia cuando las operaciones de tratamiento previstas puedan infringir las disposiciones adoptadas con arreglo a la presente Directiva;

b) ordenar al responsable o encargado del tratamiento que haga conformes las operaciones de tratamiento a las disposiciones adoptadas con arreglo a la presente Directiva, si procede, de una determinada manera y dentro de un plazo especificado, en particular ordenando la rectificación o la supresión de datos personales, o la limitación de su tratamiento con arreglo al artículo 16;

c) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.

3. Cada Estado miembro dispondrá por ley que su autoridad de control tenga poderes consultivos efectivos para asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 28 y emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional y su Gobierno o, conforme al Derecho del Estado miembro, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales.

4. El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y del Estado miembro de conformidad con la Carta.

5. Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones de la presente Directiva y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir las disposiciones adoptadas con arreglo a la presente Directiva.

Artículo 48

Notificación de infracciones

Los Estados miembros dispondrán que las autoridades competentes establezcan mecanismos eficaces que fomenten la notificación confidencial de infracciones a la presente Directiva.

Artículo 49

Informe de actividad

Cada autoridad de control elaborará un informe anual sobre sus actividades, que podrá incluir una lista de los tipos de infracciones notificadas y de tipos de las sanciones impuestas. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho del Estado miembro. Se pondrán a disposición del público, de la Comisión y del Comité Europeo de Protección de Datos.

CAPÍTULO VII

Cooperación

Artículo 50

Asistencia mutua

1. Los Estados miembros dispondrán que sus autoridades de control se faciliten entre sí información útil y se presten asistencia mutua a fin de aplicar la presente Directiva de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo consultas, inspecciones e investigaciones.

2. Los Estados miembros dispondrán que cada autoridad de control adopte todas las medidas apropiadas requeridas para responder a la solicitud de otra autoridad de control sin dilación indebida y a más tardar en el plazo de un mes tras haber recibido la solicitud. Dichas medidas podrán incluir, en particular, la transmisión de información pertinente sobre el desarrollo de una investigación.

3. Las solicitudes de asistencia deberán contener toda la información necesaria, entre otras cosas respecto de la finalidad y los motivos de la solicitud. La información que se intercambie se utilizará únicamente para el fin para el que haya sido solicitada.

4. La autoridad de control requerida no podrá negarse a responder a una solicitud, salvo si:

a) no es competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita, o

b) el hecho de atender la solicitud infringiría la presente Directiva o el Derecho de la Unión o del Estado miembro al que esté sujeta la autoridad de control que haya recibido la solicitud.

5. La autoridad de control requerida informará a la autoridad de control requirente de los resultados obtenidos o, en su caso, de los progresos registrados o de las medidas adoptadas para responder a su solicitud. La autoridad de control requerida explicará los motivos de su negativa a responder a una solicitud al amparo del apartado 4.

6. Como norma general, las autoridades de control requeridas facilitarán la información solicitada por otras autoridades de control por vía electrónica, utilizando un formato normalizado.

7. Las autoridades de control requeridas no cobrarán tasa alguna por las medidas adoptadas a raíz de una solicitud de asistencia mutua. Las autoridades de control podrán convenir normas de indemnización recíproca por gastos específicos derivados de la prestación de asistencia mutua en circunstancias excepcionales.

8. La Comisión podrá especificar, mediante actos de ejecución, 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 Comité Europeo de Protección de Datos. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 58, apartado 2.

Artículo 51

Funciones del Comité Europeo de Protección de Datos

1. El Comité Europeo de Protección de Datos creado por el Reglamento (UE) 2016/679 ejercerá, dentro del ámbito de aplicación de la presente Directiva, las siguientes funciones en relación con el tratamiento de datos:

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 de la presente Directiva;

b) examinará, a iniciativa propia o a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación de la presente Directiva, y emitirá directrices, recomendaciones y buenas prácticas, a fin de promover la aplicación coherente de la presente Directiva;

c) formulará directrices para las autoridades de control, relativas a la aplicación de las medidas contempladas en el artículo 47, apartados 1 y 3;

d) emitirá directrices, recomendaciones y buenas prácticas, con arreglo a la letra b) del presente párrafo a fin de establecer las violaciones de la seguridad de los datos personales y determinar la dilación indebida que contempla el artículo 30, apartados 1 y 2, así como las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales;

e) emitirá directrices, recomendaciones y buenas prácticas, con arreglo a la letra b) del presente párrafo en cuanto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales vaya a tener como resultado un alto riesgo para los derechos y libertades de las personas físicas a tenor del artículo 31, apartado 1;

f) examinará la aplicación práctica de las directrices, recomendaciones y buenas prácticas contempladas en las letras b) y c);

g) facilitará a la Comisión un dictamen para evaluar la adecuación del nivel de protección en un tercer país, un territorio o uno o varios sectores específicos en un tercer país o una organización internacional, incluso para evaluar si dicho tercer país, territorio, sector específico u organización internacional han dejado de garantizar un nivel de protección adecuado;

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

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

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

Respecto del párrafo primero, letra g), la Comisión facilitará al Comité Europeo de Protección de Datos toda la documentación necesaria, incluida la correspondencia con el gobierno del tercer país, el territorio o el sector específico en dicho tercer país, o la organización internacional.

2. Cuando la Comisión solicite asesoramiento del Comité Europeo de Protección de Datos podrá señalar un plazo teniendo en cuenta la urgencia del asunto.

3. El Comité Europeo de Protección de Datos transmitirá sus dictámenes, directrices, recomendaciones y buenas prácticas a la Comisión y al comité contemplado en el artículo 58, apartado 1, y los hará públicos.

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

CAPÍTULO VIII

Recursos, responsabilidad y sanciones

Artículo 52

Derecho a presentar una reclamación ante una autoridad de control

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, los Estados miembros dispondrán que todo interesado tenga derecho a presentar una reclamación ante una única autoridad de control, si considera que el tratamiento de sus datos personales infringe las disposiciones adoptadas en virtud de la presente Directiva.

2. Los Estados miembros dispondrán que, si la reclamación no se presenta ante la autoridad de control que sea competente según el artículo 45, apartado 1, la autoridad de control ante la que se haya presentado la reclamación la transmita a la autoridad de control competente sin dilación indebida. Se informará al interesado de la transmisión.

3. Los Estados miembros dispondrán que la autoridad de control ante la que se haya presentado la reclamación proporcione asistencia adicional a petición del interesado.

4. La autoridad de control competente informará al interesado sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de la tutela judicial en virtud del artículo 53.

Artículo 53

Derecho a la tutela judicial efectiva contra una autoridad de control

1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, los Estados miembros dispondrán que toda persona física o jurídica tenga derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control competente con arreglo al artículo 45, apartado 1, no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 52.

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

Artículo 54

Derecho a la tutela judicial efectiva contra el responsable o el encargado del tratamiento

Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control con arreglo al artículo 52, los Estados miembros reconocerán el derecho que asiste a todo interesado a la tutela judicial efectiva si considera que sus derechos establecidos en disposiciones adoptadas con arreglo a la presente Directiva han sido vulnerados como consecuencia de un tratamiento de sus datos personales no conforme con esas disposiciones.

Artículo 55

Representación de los interesados

Los Estados miembros, de conformidad con el Derecho procesal del Estado miembro, dispondrán que el interesado tenga derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro, que haya sido correctamente constituida con arreglo al Derecho del Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente la reclamación en su nombre y ejerza los derechos contemplados en los artículos 52, 53 y 54 en su nombre.

Artículo 56

Derecho a indemnización

Los Estados miembros dispondrán que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una operación de tratamiento ilícito o de cualquier acto que vulnere las disposiciones nacionales adoptadas con arreglo a la presente Directiva tenga derecho a recibir una indemnización del responsable o de cualquier autoridad competente en virtud del Derecho del Estado miembro por los daños y perjuicios sufridos.

Artículo 57

Sanciones

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

CAPÍTULO IX

Actos de ejecución

Artículo 58

Procedimiento de comité

1. La Comisión estará asistida por el comité establecido por el artículo 93 del Reglamento (UE) 2016/679. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. Cuando se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

3. Cuando se haga referencia al presente apartado, se aplicará el artículo 8 del Reglamento (UE) n.º 182/2011, en relación con su artículo 5.

CAPÍTULO X

Disposiciones finales

Artículo 59

Derogación de la Decisión Marco 2008/977/JAI

1. Queda derogada la Decisión Marco 2008/977/JAI del Consejo con efecto a partir del 6 de mayo de 2018.

2. Las referencias a la Decisión derogada que se menciona en el apartado 1 se entenderán hechas a la presente Directiva.

Artículo 60

Actos jurídicos de la Unión en vigor

Las disposiciones específicas relativas a la protección de datos personales en actos jurídicos de la Unión que entraron en vigor antes del 6 de mayo de 2016 en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, que regulen el tratamiento entre los Estados miembros y el acceso de autoridades designadas de los Estados miembros a los sistemas de información establecidos con arreglo a lo dispuesto en los Tratados en el ámbito de la presente Directiva no se verán afectadas.

Artículo 61

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

Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados por los Estados miembros antes del 6 de mayo de 2016 y que cumplan lo dispuesto en el Derecho de la Unión aplicable antes de dicha fecha seguirán en vigor hasta que sean modificados, sustituidos o revocados.

Artículo 62

Informes de la Comisión

1. A más tardar el 6 de mayo de 2022 y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión de la presente Directiva. Los informes se harán públicos.

2. En el marco de las evaluaciones y revisiones a que se refiere el apartado 1, la Comisión estudiará en particular la aplicación y el funcionamiento del capítulo V sobre la transferencia de datos personales a terceros países u organizaciones internacionales, prestando especial atención a las decisiones adoptadas en virtud del artículo 36, apartado 3, y del artículo 39.

3. A los efectos de los apartados 1 y 2, la Comisión podrá solicitar información a los Estados miembros y a las autoridades de control.

4. Al realizar las evaluaciones y revisiones a que hacen referencia los apartados 1 y 2, la Comisión tendrá en cuenta las posiciones y las conclusiones del Parlamento Europeo, del Consejo y de los demás órganos o fuentes pertinentes.

5. La Comisión presentará, si procede, las propuestas oportunas para modificar la presente Directiva, 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.

6. Antes del 6 de mayo de 2019, la Comisión revisará otros actos jurídicos adoptados por la Unión que regulen el tratamiento por parte de las autoridades competentes a los efectos expuestos en el artículo 1, apartado 1, con inclusión de los actos a que se refiere el artículo 60, a fin de evaluar la necesidad de aproximarlos a las disposiciones de la presente Directiva, y presentará, en su caso, las propuestas necesarias para modificar dichos actos para garantizar un enfoque coherente de la protección de datos personales en el ámbito de aplicación de la presente Directiva.

Artículo 63

Transposición

1. Los Estados miembros adoptarán y publicarán, a más tardar el 6 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones. Aplicarán dichas disposiciones a partir del 6 de mayo de 2018.

Cuando los Estados miembros adopten dichas disposiciones, estas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. No obstante lo dispuesto en el apartado 1, los Estados miembros podrán disponer que excepcionalmente y cuando suponga un esfuerzo desproporcionado, los sistemas de tratamiento automatizado establecidos con anterioridad al 6 de mayo de 2016 sean conformes con el artículo 25, apartado 1, antes del 6 de mayo de 2023.

3. No obstante lo dispuesto en los apartados 1 y 2 del presente artículo, en circunstancias excepcionales, un Estado miembro podrá adaptar al artículo 25, apartado 1, un sistema de tratamiento automatizado a que se refiere el apartado 2 del presente artículo dentro de un plazo determinado después del período previsto en el apartado 2 del presente artículo, si de no hacer así surgieran serias dificultades para el funcionamiento de ese sistema de tratamiento automatizado concreto. Notificará a la Comisión los motivos de esas serias dificultades así como los del período específico dentro del cual adaptará ese sistema de tratamiento automatizado concreto a lo dispuesto en el artículo 25, apartado 1. En cualquier caso, el período determinado no podrá ser posterior al 6 de mayo de 2026.

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

Artículo 64

Entrada en vigor

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

Artículo 65

Destinatarios

Los destinatarios de la presente Directiva son los Estados miembros.

Hecho en Bruselas, el 27 de abril de 2016.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*La Presidenta*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 27 de abril de 2016

relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 82, apartado 1, letra d), y su artículo 87, apartado 2, letra a),

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de texto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo ([1]),

Previa consulta al Comité de las Regiones,

De conformidad con el procedimiento legislativo ordinario ([2]),

Considerando lo siguiente:

(1) El 6 de noviembre de 2007, la Comisión adoptó la propuesta de Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record — PNR) con fines policiales. No obstante, al entrar en vigor el Tratado de Lisboa el 1 de diciembre de 2009, la propuesta de la Comisión, que en esta fecha todavía no había sido aprobada por el Consejo, quedó obsoleta.

(2) El «Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano» ([3]) insta a la Comisión a presentar una propuesta sobre la utilización de datos PNR para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves.

(3) La Comisión presentó una serie de elementos esenciales de la política de la Unión en esta materia en su Comunicación de 21 de septiembre de 2010 «Sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países».

(4) La Directiva 2004/82/CE del Consejo ([4]), regula la comunicación previa por los transportistas aéreos a las autoridades nacionales competentes de información anticipada sobre los pasajeros (datos API, por sus siglas en inglés «advance passenger information») con objeto de mejorar los controles fronterizos y combatir la inmigración ilegal.

(5) Son objetivos de la presente Directiva, entre otras cosas, garantizar la seguridad, proteger la vida y la seguridad de los ciudadanos y crear un marco jurídico para la protección de los datos PNR en lo que respecta a su tratamiento por las autoridades competentes.

(6) El uso eficaz de los datos PNR, por ejemplo comparando los datos PNR con diversas bases de datos sobre personas y objetos buscados, es necesario para, prevenir, detectar, investigar y enjuiciar de modo eficaz delitos de terrorismo y delitos graves, reforzando así la seguridad interior, para reunir pruebas y, en su caso, descubrir a los cómplices de los delincuentes y desmantelar redes delictivas.

(7) La evaluación de los datos PNR permite la identificación de personas no sospechosas de estar implicadas en delitos de terrorismo o en delitos graves antes de que un análisis de sus datos PNR indique que puedan estar

([1]) DO C 218 de 23.7.2011, p. 107.
([2]) Posición del Parlamento Europeo de 14 de abril de 2016 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 21 de abril de 2016.
([3]) DO C 115 de 4.5.2010, p. 1.
([4]) Directiva 2004/82/CE del Consejo, de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas (DO L 261 de 6.8.2004, p. 24).

implicadas en los mismos, y deban ser objeto de investigación adicional por parte de las autoridades competentes. Mediante la utilización de datos PNR es posible responder a la amenaza de delitos de terrorismo y delitos graves desde una perspectiva distinta del tratamiento de otras categorías de datos personales. Sin embargo, para garantizar que el tratamiento de datos se limite a lo necesario, el establecimiento y la aplicación de criterios de evaluación debe limitarse a los delitos de terrorismo y a la delincuencia grave para las que es pertinente el uso de esos criterios. Deben definirse, por otra parte, los criterios de evaluación de tal manera que el sistema señale al menor número posible de personas inocentes.

(8) Las compañías aéreas ya recogen y tratan datos PNR de sus pasajeros para sus fines comerciales propios. La presente Directiva no debe imponer ninguna obligación a las compañías aéreas de recoger o almacenar datos adicionales de los pasajeros ni a los pasajeros de facilitar a las compañías aéreas datos adicionales a los ya previstos.

(9) Algunas compañías aéreas almacenan los datos API que recogen como parte de los datos PNR, mientras que otras no lo hacen. Utilizar los datos PNR junto con los datos API representa un valor añadido para ayudar a los Estados miembros a verificar la identidad de una persona, reforzando así el valor policial de ese resultado y reduciendo al mínimo el riesgo de realizar controles e investigaciones de personas inocentes. Es, pues, importante asegurarse de que, cuando las compañías aéreas recojan datos API, los transfieran, con independencia de que conserven o no dichos datos por otros medios técnicos que los datos PNR.

(10) Para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves, es fundamental que todos los Estados miembros introduzcan disposiciones que impongan a las compañías aéreas que realizan vuelos exteriores de la UE, la obligación de transferir todos los datos PNR que recojan, incluidos los datos API. El Estado miembro debe tener la posibilidad también de ampliar esa obligación a las compañías aéreas que realizan vuelos interiores de la UE. Estas disposiciones se deben entender sin perjuicio de la Directiva 2004/82/CE.

(11) El tratamiento de datos personales debe ser proporcional a los objetivos específicos de seguridad que persigue la presente Directiva.

(12) La definición de delitos de terrorismo que se aplica en la presente Directiva deberá ser la misma que la de la Decisión marco 2002/475/JAI del Consejo ([1]). La definición de delitos graves deberá englobar las categorías de delito enumeradas en el anexo II de la presente Directiva.

(13) Los datos PNR deberán transmitirse a una unidad única de información sobre los pasajeros («UIP») designada en el Estado miembro de que se trate, a fin de garantizar la claridad y reducir los costes de las compañías aéreas. La UIP puede disponer de distintas sucursales dentro de un Estado miembro, y los Estados miembros también podrán establecer conjuntamente una UIP. Los Estados miembros deberán intercambiar mutuamente la información a través de las correspondientes redes de intercambio de información para facilitar dicho intercambio y garantizar la interoperabilidad.

(14) Los Estados miembros deberán sufragar los costes del uso, la conservación y el intercambio de los datos PNR.

(15) Las listas de datos PNR que deba obtener una UIP deberá elaborarse con el objetivo de reflejar las legítimas necesidades de las autoridades públicas para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves, mejorando así la seguridad interior en la Unión y la protección de los derechos fundamentales y, en particular, el derecho a la intimidad y la protección de datos personales. Para ello se deben aplicar exigencias elevadas, conforme a la Carta de los Derechos Fundamentales de la Unión Europea («la Carta»), el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal («Convenio n.º 108») y el Convenio para la protección de los derechos humanos y de las libertades fundamentales («el CEDH»). Dichas listas no deben basarse en el origen racial o étnico, religión o convicciones, opiniones políticas o de cualquier otro tipo, la pertenencia a un sindicato, la salud, vida u orientación sexual. Los datos PNR solo deben contener la información detallada sobre las reservas e itinerarios de viaje que permita a las autoridades competentes identificar a los pasajeros por vía aérea que representan una amenaza para la seguridad interior.

(16) En la actualidad se dispone de dos métodos de transferencia de datos: el método de extracción, en el que las autoridades competentes del Estado miembro que solicita los datos PNR pueden acceder al sistema de reserva de la compañía aérea y obtener («extraer») una copia de los datos PNR deseados, y el método de transmisión, en el que las compañías aéreas envían («transmiten») los datos PNR a la autoridad solicitante, lo que permite a las compañías aéreas mantener el control de los datos suministrados. Se considera que el «método de transmisión» ofrece un nivel mayor de protección de los datos y que debe ser obligatorio para todas las compañías aéreas.

([1]) Decisión marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo (DO L 164 de 22.6.2002, p. 3).

(17) La Comisión apoya las directrices de la Organización de Aviación Civil Internacional (OACI) sobre los datos PNR. Estas directrices deben, por ello, ser la base para adoptar los formatos de datos admitidos para la transmisión de datos PNR por las compañías aéreas a los Estados miembros. A fin de garantizar condiciones uniformes de ejecución de los formatos de datos admitidos y de los protocolos aplicables a la transferencia de datos de las compañías aéreas, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([1]).

(18) Los Estados miembros deben tomar todas las medidas necesarias para que las compañías aéreas puedan cumplir sus obligaciones con arreglo a la presente Directiva. Los Estados miembros deben imponer sanciones efectivas, proporcionadas y disuasorias, incluidas las pecuniarias, a las compañías aéreas que incumplan sus obligaciones de transmisión de datos PNR.

(19) Cada Estado miembro debe ser responsable de evaluar las posibles amenazas relacionadas con los delitos de terrorismo y los delitos graves.

(20) Tomando plenamente en consideración el derecho a la protección de datos personales y el derecho a la no discriminación, no debe tomarse ninguna decisión que pudiera tener efectos jurídicos adversos para una persona o afectarle gravemente en razón únicamente del tratamiento automatizado de datos PNR. Asimismo, con arreglo a los artículos 8 y 21 de la Carta, dichas decisiones deben evitar toda discriminación por motivos como el sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual. La Comisión debe tener también en cuenta estos principios cuando revise la aplicación de la presente Directiva.

(21) Los Estados miembros no podrán en ningún caso utilizar el resultado del tratamiento de datos PNR como razón para eludir sus obligaciones internacionales en virtud de la Convención de Ginebra sobre el Estatuto de los Refugiados de 28 de julio de 1951, modificada por el Protocolo de 31 de enero de 1967, ni para negar a los solicitantes de asilo unas vías jurídicas seguras y efectivas de acceso al territorio de la Unión con vistas a ejercer su derecho a la protección internacional.

(22) Teniendo plenamente en cuenta los principios de la jurisprudencia reciente expuesta por el Tribunal de Justicia de la Unión Europea, la aplicación de la presente Directiva debe garantizar el pleno respeto de los derechos fundamentales y el derecho a la intimidad, así como el principio de proporcionalidad. Asimismo, debe responder realmente a los objetivos de necesidad y proporcionalidad para favorecer los intereses generales reconocidos por la Unión y a la necesidad de proteger los derechos y libertades de los demás en la lucha contra el terrorismo y la delincuencia grave. La presente Directiva debe aplicarse cuando exista una justificación suficiente y deben preverse las garantías necesarias para asegurar la legalidad de cualquier tipo de almacenamiento, análisis, uso o transferencia de datos PNR.

(23) Los Estados miembros deben intercambiar y a través de Europol los datos PNR que reciban cuando ello se considere necesario para la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo o delitos graves. Las UIP deben transmitir, cuando proceda y sin demora, los resultados del tratamiento de datos PNR a las de otros Estados miembros, para ulterior investigación. Las disposiciones de la presente Directiva se entienden sin perjuicio de otros instrumentos de la Unión relativos al intercambio de información entre la policía u otras autoridades policiales y las judiciales, incluida la Decisión 2009/371/JAI del Consejo ([2]), y la Decisión marco 2006/960/JAI ([3]). Este intercambio de datos PNR entre las autoridades policiales y judiciales debe regirse por las normas de cooperación policial y judicial y no socavar el alto nivel de protección de la intimidad y de los datos personales exigido por la Carta, el Convenio n.º 108 y el CEDH.

(24) Debe garantizarse el intercambio seguro de información sobre datos PNR entre los Estados miembros a través de cualquiera de los canales existentes de cooperación entre las autoridades competentes de los Estados miembros, así como en particular con Europol a través de la Aplicación Segura de la red de Intercambio de Información (SIENA) de Europol.

([1]) Reglamento (UE) n.º 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).

([2]) Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol) (DO L 121 de 15.5.2009, p. 37).

([3]) Decisión marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea (DO L 386 de 29.12.2006, p. 89).

(25) El período durante el cual deben conservarse los datos PNR debe ser el necesario y debe ser proporcional a las finalidades de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves. Dada la naturaleza de los datos y su utilización, es necesario que los datos PNR se conserven durante un período suficientemente largo para realizar análisis y utilizarlos en las investigaciones. Para evitar una utilización desproporcionada es necesario que, después del período inicial de conservación, los datos PNR se despersonalicen mediante enmascaramiento de elementos de los datos Con el fin de garantizar el más alto nivel de protección de datos, el acceso al conjunto total de datos PNR, que permiten la identificación directa del interesado, solo debe poder autorizarse en condiciones muy estrictas y limitadas tras dicho período inicial.

(26) Cuando se hayan transmitido datos PNR específicos a las autoridades competentes y estos se utilicen en el contexto de un enjuiciamiento o de investigaciones penales específicos, la conservación de dichos datos por las autoridades competentes debe regirse por el derecho nacional, con independencia de los períodos de conservación de datos fijados en la presente Directiva.

(27) En cada Estado miembro, el tratamiento de los datos PNR por la UIP y las autoridades competentes debe respetar normas de protección de datos personales previstos en el derecho nacional que sean conformes con la Decisión marco 2008/977/JAI del Consejo ([1]), así como los requisitos específicos de protección de datos establecidos en la presente Directiva. Las referencias a la Decisión marco 2008/977/JAI, deberán entenderse como hechas a la legislación actualmente en vigor, así como a la legislación que la sustituya.

(28) Considerando el derecho a la protección de datos personales, los derechos de los interesados relativos al tratamiento de sus datos PNR, tales como los derechos de acceso, rectificación, supresión y restricción de los datos PNR y el derecho a una indemnización y a una reparación judicial, deber ser conformes tanto con la Decisión marco 2008/977/JAI como con el alto nivel de protección brindado por la Carta y el CEDH.

(29) Teniendo en cuenta el derecho de los pasajeros a ser informados del tratamiento de sus datos personales, los Estados miembros debe garantizar que los pasajeros reciban información precisa, de fácil acceso y comprensión, sobre la recogida de datos PNR y su transferencia a la UIP, así como sus derechos como interesados.

(30) La presente Directiva se entiende sin perjuicio del derecho de la Unión y nacional relativo al principio de acceso público a los documentos oficiales.

(31) Las transferencias de datos PNR por los Estados miembros a los terceros países deber permitirse solo caso por caso y respetando plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la Decisión marco 2008/977/JAI. Para garantizar la protección de datos personales, dichas transferencias debe cumplir requisitos adicionales relativos a la finalidad de la transferencia. También deben de estar sujetas a los principios de necesidad y proporcionalidad y al elevado nivel de protección que brindan la Carta y el CEDH.

(32) La autoridad nacional de control establecida en aplicación de la Decisión marco 2008/977/JAI también debe ser responsable de asesorar sobre y vigilar la aplicación de las disposiciones adoptadas por los Estados miembros de conformidad con la presente Directiva.

(33) La presente Directiva no afecta a la posibilidad de que los Estados miembros establezcan en su derecho nacional un mecanismo para recoger y tratar los datos PNR proporcionados por operadores económicos que no sean compañías aéreas, tales como agencias de viaje y operadores turísticos que prestan servicios relacionados con los viajes, como la reserva de vuelos, para los cuales recogen y tratan datos PNR, o de los transportistas que no sean los mencionados en él, siempre que ele derecho nacional de que se trate respete el derecho de la Unión.

(34) La presente Directiva se entiende sin perjuicio de las normas vigentes de la Unión sobre la forma en que se realizan los controles de fronteras ni de las normas de la Unión que rigen la entrada y salida de su territorio.

(35) Como consecuencia de las diferencias jurídicas y técnicas entre las disposiciones nacionales sobre el tratamiento de datos personales, incluidos los datos PNR, las compañías aéreas se enfrentan y se enfrentarán a requisitos diferentes en cuanto al tipo de información que deben transmitir y a las condiciones en que deben facilitársela a

([1]) 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).

las autoridades nacionales competentes. Estas diferencias pueden ir en detrimento de una cooperación efectiva entre las autoridades nacionales competentes a efectos de prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves. Por ello es necesario establecer a escala de la Unión un marco legal común para la transferencia y tratamiento de datos PNR.

(36) La presente Directiva respeta los derechos fundamentales y los principios de la Carta, y en particular el derecho de protección de datos de carácter personal, el derecho a la intimidad y el derecho a la no discriminación reconocidos en los artículos 8, 7 y 21 de la misma, y debe aplicarse en consecuencia. La presente Directiva es compatible con los principios de protección de datos y sus disposiciones se ajustan a la Decisión marco 2008/977/JAI del Consejo. Además, con el fin de cumplir el principio de proporcionalidad, la presente Directiva, en determinadas materias, contiene normas de protección de datos más estrictas que la Decisión marco 2008/977/JAI.

(37) Se ha limitado en lo posible el alcance de la presente Directiva pues permite conservar los datos PNR durante un período máximo de 5 años, tras el cual los datos deberán suprimirse; dispone que los datos deben despersonalizarse mediante enmascaramiento de los elementos de los datos tras un período inicial de seis meses, y prohíbe la recogida y utilización de datos sensibles. Para garantizar la eficiencia y un alto nivel de protección de datos, se exige a los Estados miembros que garanticen que una autoridad nacional de control independiente y, en particular, un responsable de la protección de datos, sea responsable de asesorar y de supervisar el modo en que se tratan los datos PNR. Cualquier tratamiento de datos PNR deberá registrarse o documentarse a efectos de la verificación de su legalidad, de autocontrol, así como para garantizar adecuadamente la integridad y seguridad del tratamiento. Los Estados miembros también deberán asegurarse de que los pasajeros reciban una información clara y precisa sobre la recogida de datos PNR y sobre sus derechos.

(38) Dado que los objetivos de la presente Directiva, a saber, la transferencia de datos PNR por las compañías aéreas y su tratamiento a efectos de prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y la delincuencia grave, no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos.

(39) De conformidad con el artículo 3 del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, estos Estados miembros han notificado su deseo de participar en la adopción y aplicación de la presente Directiva.

(40) De conformidad con los artículos 1 y 2 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participa en la adopción de la presente Directiva y no queda vinculada por la misma ni sujeta a su aplicación.

(41) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo ([1]), emitió su dictamen el 25 de marzo de 2011.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

Disposiciones generales

Artículo 1

Objeto y ámbito de aplicación

1. La presente Directiva regula:

a) la transferencia por las compañías aéreas de datos del registro de nombres de los pasajeros (PNR) de vuelos exteriores de la UE;

b) el tratamiento de los datos a que se refiere la letra a), incluida su recogida, utilización y conservación por los Estados miembros, así como el intercambio de los mismos entre dichos Estados miembros.

([1]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

2. Los datos PNR obtenidos con arreglo a la presente Directiva podrán tratarse únicamente con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves contemplados en el artículo 6, apartado 2, letras a), b) y c).

Artículo 2

Aplicación de la presente Directiva a los vuelos interiores de la UE

1. En caso de que un Estado miembro decida aplicar la presente Directiva a los vuelos interiores de la UE, lo notificará por escrito a la Comisión. Cualquier Estado miembro podrá efectuar o revocar esta notificación en cualquier momento. La Comisión publicará dicha notificación y cualquier revocación de la misma en el *Diario Oficial de la Unión Europea*.

2. Cuando se efectúe la notificación a que se refiere el apartado 1, todas las disposiciones de la presente Directiva se aplicarán a los vuelos interiores de la UE de igual modo que si se tratara de vuelos al exterior de la UE, y a los datos PNR de vuelos interiores de la UE de igual modo que si se tratara de datos PNR de vuelos al exterior de la UE.

3. Cada Estado miembro podrá decidir aplicar la presente Directiva exclusivamente a vuelos interiores de la UE seleccionados. Al adoptar tal decisión, el Estado miembro deberá elegir los vuelos que considere necesarios a fin de perseguir los objetivos de la presente Directiva. El Estado miembro podrá decidir modificar la selección de vuelos interiores de la UE en todo momento.

Artículo 3

Definiciones

A efectos de la presente Directiva, se entenderá por:

1) «compañía aérea»: empresa de transporte aéreo con una licencia de explotación válida o similar que le permita llevar a cabo el transporte de pasajeros por vía aérea;

2) «vuelo exterior de la UE»: cualquier vuelo, programado o no programado por una compañía aérea, procedente de un tercer país que tenga previsto aterrizar en el territorio de un Estado miembro o volar procedente del territorio de un Estado miembro y que tenga previsto aterrizar en un tercer país, incluidos en ambos casos los vuelos que hagan escala en el territorio de Estados miembros o de terceros países;

3) «vuelo interior de la UE»: cualquier vuelo, programado o no programado por una compañía aérea, procedente del territorio de un Estado miembro y que tenga previsto aterrizar en el territorio de otro u otros Estados miembros, sin escalas en el territorio de un tercer país;

4) «pasajero»: toda persona, incluidos los pasajeros en tránsito o en conexión y exceptuados los miembros de la tripulación, transportada o que vaya a ser transportada a bordo de una aeronave con el consentimiento de la compañía aérea, lo cual se manifiesta en la inclusión de la persona en la lista de pasajeros;

5) «registro de nombres de los pasajeros» o «PNR»: una relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información necesaria para el tratamiento y el control de las reservas por parte de las compañías aéreas que las realizan y participan en el sistema PNR, por cada viaje reservado por una persona o en su nombre, ya estén contenidos en sistemas de reservas, en sistemas de control de salidas utilizado para embarcar a los pasajeros en el vuelo o en sistemas equivalentes que posean las mismas funcionalidades;

6) «sistema de reserva»: el sistema de reservas interno de la compañía aérea en el cual se recogen los datos PNR para el tratamiento de las reservas;

7) «método de transmisión»: método por el cual las compañías aéreas envían los datos PNR incluidos en el anexo I a la base de datos de la autoridad requirente;

8) «delitos de terrorismo»: los delitos con arreglo al derecho nacional a que se refieren los artículos 1 a 4 de la Decisión marco 2002/475/JAI;

9) «delitos graves»: los delitos incluidos en el anexo II que son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no inferior a tres años con arreglo al derecho nacional de un Estado miembro;

10) «despersonalizar mediante enmascaramiento de elementos de los datos»: hacer invisibles para un usuario aquellos elementos de los datos que servirían para identificar directamente al interesado.

CAPÍTULO II

Responsabilidades de los estados miembros

Artículo 4

Unidad de Información sobre los Pasajeros

1. Cada Estado miembro establecerá o designará una autoridad competente para la prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo y delitos graves, o una sucursal de esa autoridad, para actuar como su Unidad de Información sobre los Pasajeros («UIP»).

2. La UIP será responsable de:

a) recoger los datos PNR de las compañías aéreas, almacenar y procesar esos datos y transferir dichos datos o el resultado de su tratamiento a las autoridades competentes a que hace mención el artículo 7;

b) intercambiar tanto los datos PNR como de los resultados de su tratamiento con las UIP de otros Estados miembros y con Europol, de conformidad con los artículos 9 y 10.

3. El personal de la UIP podrá ser enviado en comisión de servicios por las autoridades competentes. Los Estados miembros dotarán a las UIP de los recursos adecuados para que realicen su cometido.

4. Dos o más Estados miembros (los Estados miembros participantes) podrán establecer o designar una autoridad única para que actúe como su UIP. Esta UIP se establecerá en uno de los Estados miembros participantes y se considerará la UIP de todos los Estados miembros participantes. Los Estados miembros participantes acordarán conjuntamente las normas detalladas de funcionamiento de la UIP y respetarán los requisitos establecidos en la presente Directiva.

5. En el plazo de un mes desde la creación de su UIP, cada Estado miembro se lo notificará a la Comisión, y podrá modificar su notificación en cualquier momento. La Comisión publicará la notificación, y sus eventuales modificaciones, en el *Diario Oficial de la Unión Europea*.

Artículo 5

Responsable de la protección de datos en la UIP

1. La UIP designará a un responsable de la protección de datos para controlar el tratamiento de los datos PNR y aplicar las garantías oportunas.

2. Los Estados miembros dotarán al responsable de la protección de datos de los medios necesarios para que desempeñe sus funciones y cometidos con arreglo al presente artículo de manera eficaz e independiente.

3. Los Estados miembros velarán por que el interesado tenga derecho a ponerse en contacto con el responsable de la protección de datos, como punto de contacto único, para todas las cuestiones relacionadas con el tratamiento de sus datos PNR.

Artículo 6

Tratamiento de los datos PNR

1. Los datos PNR transmitidos por las compañías aéreas serán recopilados por la UIP del Estado miembro que corresponda, con arreglo a lo dispuesto en el artículo 8. Si los datos PNR transmitidos por las compañías aéreas incluyeran datos distintos de los enumerados en el anexo I, la UIP los suprimirá inmediatamente y de manera definitiva en el momento de su recepción.

2. La UIP tratará los datos PNR solo para realizar:

a) una evaluación de los pasajeros antes de su llegada o salida programada del Estado miembro, a fin de identificar a toda persona que deba ser examinada de nuevo por las autoridades competentes a que se refiere el artículo 7 y, en su caso, por Europol, de conformidad con el artículo 10, ante la posibilidad de que pudiera estar implicada en un delito de terrorismo o delito grave;

b) responder en cada caso particular, a las peticiones debidamente razonadas y con suficiente base de las autoridades competentes de que se suministren y traten datos PNR en casos específicos a efectos de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, y facilitar a las autoridades competentes o, en su caso, a Europol, los resultados de dicho tratamiento, y

c) analizar los datos PNR con el fin de actualizar o establecer nuevos criterios que deben utilizarse en las evaluaciones realizadas en virtud del apartado 3, letra b), a fin de identificar a toda persona que pueda estar implicada en un delito de terrorismo o delito grave.

3. Al realizar la evaluación a que se refiere el artículo 2, letra a), la UIP podrá:

a) comparar los datos PNR con las bases de datos pertinentes a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, incluidas las bases de datos sobre personas u objetos buscados o bajo alerta, de acuerdo con las normas de la Unión, internacionales y nacionales aplicables a dichas bases de datos, o

b) tratar los datos PNR con arreglo a criterios predeterminados.

4. La evaluación de los pasajeros antes de su llegada o salida programada del Estado miembro mencionado, efectuada de conformidad con los criterios predeterminados a que se refiere a que se refiere el apartado 3, la letra b), se realizará de forma no discriminatoria con arreglo a criterios de evaluación establecidos por su UIP. Estos criterios predeterminados de evaluación deben ser orientados, proporcionados y específicos. Los Estados miembros se asegurarán de que las UIP establezcan esos criterios y los revisen periódicamente, en cooperación con las autoridades competentes mencionadas en el artículo 7. Los criterios no se basarán en ningún caso en el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud o la vida u orientación sexual de la persona.

5. Los Estados miembros velarán por que se revise individualmente, por medios no automatizados, todo resultado positivo que arroje el tratamiento automatizado de los datos PNR efectuado con arreglo al artículo 2, letra a), con el fin de comprobar si es necesario que las autoridades competentes a que hace referencia el artículo 7 emprendan una acción en virtud del derecho nacional.

6. La UIP de un Estado miembro transmitirá los datos PNR de las personas identificadas con arreglo al apartado 2, letra a), o los resultados del tratamiento de esos datos PNR a las autoridades competentes pertinentes a que hace referencia el artículo 7 del mismo Estado miembro para su ulterior examen. Dicha transmisión solo se llevará a cabo tras un análisis de cada caso y, en caso de tratamiento automatizado de los datos PNR, tras una revisión individualizada por medios no automatizados.

7. Los Estados miembros velarán por que el responsable de la protección de datos tenga acceso a todos los datos tratados por la UIP. Si el responsable de la protección de datos considera que el tratamiento de un dato cualquiera no ha sido lícito, podrá remitirlo a la autoridad nacional de control.

8. El almacenamiento, el tratamiento y análisis de los datos PNR por parte de la UIP se realizará exclusivamente en uno o varios lugares seguros, dentro del territorio de los Estados miembros.

9. Las consecuencias de las evaluaciones de los pasajeros a que se refiere la letra a) del apartado 2 del presente artículo no perjudicarán el derecho de entrada de las personas que gocen del derecho de la Unión de libre circulación en el territorio del Estado miembro en cuestión tal como se establece en la Directiva 2004/38/CE del Parlamento Europeo y del Consejo ([1]). Por otra parte, en caso de que se efectúen en relación con vuelos interiores de la UE entre Estados miembros a los que sea aplicable el Reglamento (CE) n.º 562/2006 del Parlamento Europeo y del Consejo ([2]), las consecuencias de tales evaluaciones se ajustarán a dicho Reglamento.

Artículo 7

Autoridades competentes

1. Cada Estado miembro elaborará la lista de autoridades competentes para solicitar o recibir datos PNR o el resultado del tratamiento de los mismos de las UIP, a fin de seguir examinando esa información o de tomar las medidas adecuadas para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves.

2. Las autoridades a que se refiere el apartado 1 serán del Estado miembro competentes para la prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo y delitos graves.

3. A efectos del artículo 9, apartado 3, cada Estado miembro notificará a la Comisión la lista de sus autoridades competentes a la Comisión antes del 25 de mayo de 2017, y podrá modificar su notificación en todo momento. La Comisión publicará la notificación, y sus eventuales modificaciones, en el *Diario Oficial de la Unión Europea*.

4. Los datos PNR y los resultados del tratamiento de dichos datos recibidos por la UIP podrán ser objeto de tratamiento posterior por las autoridades competentes de los Estados miembros únicamente con el fin específico de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.

5. El apartado 4 se entiende sin perjuicio de las facultades policiales o judiciales con arreglo al derecho nacional en el caso de que, en el curso de la acción ejercida después del tratamiento, se detecten otros delitos o indicios de delitos.

6. Las autoridades competentes no adoptarán ninguna decisión que produzca efectos jurídicos adversos para una persona o que afecte significativamente a una persona únicamente en razón del tratamiento automatizado de datos PNR. Dichas decisiones no deberán basarse en la raza o el origen étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud o la vida u orientación sexual de la persona.

Artículo 8

Obligaciones de las compañías aéreas en relación con la transmisión de datos

1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las compañías aéreas envíen, mediante el método de transmisión, los datos PNR relacionados en el anexo I, en la medida en que ya los hayan recopilado en el transcurso normal de su actividad, a la base de datos de la UIP del Estado miembro en cuyo territorio aterrizará o de cuyo territorio saldrá el vuelo. En los casos en que el código de un vuelo internacional sea compartido con una o más compañías aéreas, la obligación de transmitir los datos PNR de todos los pasajeros de dicho vuelo recaerá en la compañía aérea que explote el vuelo. Si un vuelo exterior de la UE realiza una o varias escalas en los aeropuertos de los Estados miembros, las compañías aéreas transmitirán los datos PNR de todos los pasajeros a las UIP de todos los Estados miembros interesados. Lo mismo se aplica a los vuelos interiores de la UE con una o varias escalas en aeropuertos de diversos Estados miembros, pero solo en relación con los Estados miembros que estén recogiendo datos PNR de vuelos interiores de la UE.

([1]) Directiva 2004/38/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al derecho de los ciudadanos de la Unión y de los miembros de sus familias a circular y residir libremente en el territorio de los Estados miembros por la que se modifica el Reglamento (CEE) n.º 1612/68 y se derogan las Directivas 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE y 93/96/CEE (DO L 158 de 30.4.2004, p. 77).

([2]) Reglamento (CE) n.º 562/2006 del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, por el que se establece un Código comunitario de normas para el cruce de personas por las fronteras (Código de fronteras Schengen) (DO L 105 de 13.4.2006, p. 1).

2. En caso de que las compañías aéreas hayan recopilado los datos de información anticipada sobre los pasajeros (API, por sus siglas en inglés de «*advance passenger information*») enumerados en el punto 18 del anexo I, pero no los conserven con los mismos medios técnicos que otros datos PNR, los Estados miembros adoptarán las medidas necesarias para garantizar que las compañías aéreas envíen también esos datos, mediante el método de transmisión, a la UIP del Estado miembro a que se refiere el apartado 1. En caso de que se lleve a cabo esta transmisión, se aplicarán todas las disposiciones de la presente Directiva en relación con los mencionados datos API.

3. Las compañías aéreas transmitirán los datos PNR por medios electrónicos utilizando los protocolos y los formatos de datos comunes que deberán adoptarse conforme al procedimiento de examen a que se refiere el artículo 17, apartado 2 o, en caso de fallo técnico, por cualquier otro medio apropiado que garantice un nivel adecuado de seguridad de los datos:

a) 24 a 48 horas antes de la hora de salida programada del vuelo, e

b) inmediatamente después del cierre del vuelo, es decir, una vez que los pasajeros hayan embarcado en el avión en preparación de la salida y no sea posible embarcar o desembarcar pasajeros.

4. Los Estados miembros permitirán a las compañías aéreas que limiten la transmisión a que se refiere el apartado 3, letra b), a actualizaciones de la transmisión a que se refiere la letra a) de dicho apartado.

5. Cuando sea necesario acceder a los datos PNR para responder a una amenaza concreta y real relacionada con delitos de terrorismo o delitos graves, las compañías aéreas, caso por caso, transmitirán los datos PNR en momentos distintos de los mencionados en el apartado 3, a petición de una UIP y de conformidad con el derecho nacional.

Artículo 9

Intercambio de información entre Estados miembros

1. En lo que respecta a las personas identificadas por una UIP de conformidad con el artículo 6, apartado 2, los Estados miembros garantizarán que todos los datos PNR pertinentes y necesarios, o el resultado de su tratamiento, sean transmitidos por la UIP en cuestión a las unidades correspondientes de los demás Estados miembros. Las UIP de los Estados miembros receptores remitirán la información recibida, de conformidad con el artículo 6, apartado 6, a sus autoridades competentes.

2. La UIP de un Estado miembro tendrá derecho a solicitar, en caso necesario, a la UIP de cualquier otro Estado miembro que le suministre los datos PNR almacenados en la base de datos de esta última y que aún no hayan sido despersonalizados mediante enmascaramiento de elementos de los datos, de conformidad con el artículo 12, apartado 2, así como, si fuera necesario, el resultado de cualquier tratamiento de los mismos, si este ya se hubiera realizado de conformidad con el artículo 6, apartado 2, letra a). La solicitud deberá ser debidamente motivada. Podrá basarse en cualquier elemento de los datos o en una combinación de los mismos, según estime necesario la UIP solicitante en cada caso concreto para la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo o delitos graves. Las UIP deberán proporcionar la información solicitada lo antes posible. En caso de que los datos solicitados hayan sido despersonalizados mediante enmascaramiento de elementos de los datos de conformidad con el artículo 12, apartado 2, la UIP únicamente deberá proporcionar los datos PNR completos cuando crea razonablemente que es necesario a los efectos a que se refiere el artículo 6, apartado 2, letra b), y solo cuando lo haya autorizado una autoridad competente conforme a lo dispuesto en el artículo 12, apartado 3, letra b).

3. Las autoridades competentes de un Estado miembro pueden solicitar directamente a la UIP de cualquier otro Estado miembro que les facilite los datos PNR almacenados en la base de datos de este último únicamente cuando sea necesario en casos de urgencia y en las condiciones establecidas en el apartado 2. Las solicitudes de las autoridades competentes deberán ser motivadas. Siempre se enviará una copia de ellas a la UIP del Estado miembro solicitante, En todos los demás casos las autoridades competentes canalizarán sus solicitudes a través de la UIP de su propio Estado miembro.

4. Excepcionalmente, cuando sea necesario acceder a los datos PNR para responder a una amenaza concreta y real relacionada con delitos de terrorismo o delitos graves, la UIP de un Estado miembro tendrá derecho a solicitar a la UIP de otro Estado miembro acceder a datos PNR, de conformidad con el artículo 8, apartado 5, y facilitarlos a la UIP solicitante.

5. El intercambio de información previsto en el presente artículo podrá realizarse utilizando cualquiera de las vías existentes de cooperación entre las autoridades competentes de los Estados miembros. Para la solicitud y el intercambio

de información se utilizará la lengua aplicable a la vía de cooperación utilizada. Los Estados miembros, al efectuar sus notificaciones de conformidad con el artículo 4, apartado 5, informarán también a la Comisión de los puntos de contacto a los que se podrán enviar las solicitudes en caso de emergencia. La Comisión comunicará estos detalles a los Estados miembros.

Artículo 10

Condiciones de acceso de Europol a los datos PNR

1. Europol tendrá derecho a solicitar datos PNR o el resultado del procesamiento de dichos datos a las UIP de los Estados miembros dentro de los límites de sus competencias y para el desempeño de sus funciones.

2. Europol podrá dirigir, caso por caso, a la UIP de cualquier Estado miembro, a través de la unidad nacional de Europol, una solicitud electrónica debidamente motivada de transmisión de datos PNR específicos o del resultado del tratamiento de los mismos. Europol podrá dirigir dicha solicitud cuando sea estrictamente necesario para apoyar y reforzar la acción de los Estados miembros a efectos de prevenir, detectar o investigar un delito de terrorismo específico o delitos graves, siempre que el delito entre dentro de las competencias de Europol de conformidad con la Decisión 2009/371/JAI. La solicitud indicará las causas razonables por las que Europol considera que la transmisión de los datos PNR o de los resultados de su tratamiento va a contribuir significativamente a prevenir, detectar o investigar la infracción penal en cuestión.

3. Europol informará al responsable de la protección de datos designado de conformidad con el artículo 28 de la Decisión 2009/371/JAI de cada uno de los intercambios de información en virtud del presente artículo.

4. El intercambio de información en virtud del presente artículo se realizará a través de SIENA y de conformidad con la Decisión 2009/371/JAI. Para la solicitud y el intercambio de información se utilizará la lengua aplicable a SIENA.

Artículo 11

Transferencias de datos a los terceros países

1. Un Estado miembro podrá transmitir a un tercer país los datos PNR y el resultado del tratamiento de dichos datos conservados por la UIP con arreglo al artículo 12 en casos concretos y si:

a) se cumplen las condiciones establecidas en el artículo 13 de la Decisión marco 2008/977/JAI;

b) la transmisión es necesaria para los fines de la presente Directiva a que se refiere el artículo 1, apartado 2;

c) el tercer país acuerda transmitir los datos a otro tercer país únicamente si fuera estrictamente necesario para los fines de la presente Directiva a que se refiere el artículo 1, apartado 2, y solo con la autorización expresa del Estado miembro, y

d) se reúnen unas condiciones idénticas a las establecidas en el artículo 9, apartado 2.

2. No obstante lo dispuesto en el artículo 13, apartado 2 de la Decisión marco 2008/977/JAI, las transmisiones de datos PNR sin consentimiento previo del Estado miembro del que fueron obtenidos los datos, se permitirán en circunstancias excepcionales y solamente si:

a) son esenciales para responder a una amenaza específica y real relacionada con delitos de terrorismo o delitos graves de un Estado miembro o de un tercer país, y

b) el consentimiento previo no puede obtenerse a su debido tiempo.

Se informará sin demora a la autoridad responsable de dar el consentimiento y la transmisión se registrará debidamente y podrá ser objeto de una verificación posterior.

3. Los Estados miembros transmitirán datos PNR a las autoridades competentes de terceros países únicamente en condiciones acordes con la presente Directiva y exclusivamente después de asegurarse de que la utilización de los datos PNR prevista por los receptores se ajusta a dichas condiciones y garantías.

4. Se informará al responsable de la protección de datos del Estado miembro que haya transmitido los datos PNR cada vez que el Estado miembro transfiera datos PNR en virtud del presente artículo.

Artículo 12

Período de conservación de los datos y despersonalización

1. Los Estados miembros se asegurarán de que los datos PNR proporcionados por las compañías aéreas a la UIP se conservan en una base de datos de la Unidad durante un plazo de cinco años a partir de su transmisión a la UIP del Estado miembro en cuyo territorio tenga su punto de aterrizaje u origen el vuelo.

2. Al finalizar un plazo de seis meses desde la transmisión de datos PNR mencionada en el apartado 1, todos los datos PNR deberán ser despersonalizados mediante enmascaramiento de los siguientes elementos que podrían servir para identificar directamente al pasajero al que se refieren los datos PNR:

a) nombre(s) y apellido(s), incluidos los de otros pasajeros que figuran en el PNR y número de personas que figuran en el PNR que viajan juntas;

b) dirección y datos de contacto;

c) rodos los datos sobre el pago, incluida la dirección de facturación, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, o a cualquier otra persona;

d) información sobre viajeros asiduos;

e) observaciones generales, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, y

f) toda la API recopilada.

3. Al finalizar el período de seis meses mencionado en el apartado 2, solo se permitirá la divulgación de los datos PNR completos cuando:

a) se crea razonablemente que es necesario a los efectos establecidos en el artículo 6, apartado 2, letra b), y

b) haya sido aprobado por:

   i) una autoridad judicial, u

   ii) otra autoridad nacional competente para verificar si se cumplen las condiciones para la divulgación conforme al derecho nacional, con sujeción a la información y revisión *a posteriori* del responsable de la protección de datos de la UIP.

4. Los Estados miembros se asegurarán de que los datos PNR sean suprimidos de modo permanente al finalizar el período a que se refiere el apartado 1. Esta obligación se entenderá sin perjuicio de aquellos casos en que se hayan transferido datos PNR específicos a una autoridad competente y se estén utilizando en el marco de un asunto específico a efectos de prevenir, detectar, investigar o enjuiciar los actos de terrorismo o delitos graves, en cuyo caso la conservación de los datos por la autoridad competente se regirá por el derecho nacional.

5. Los resultados del tratamiento a que se refiere el artículo 6, apartado 2, letra a), serán conservados por laUIP únicamente durante el tiempo necesario para informar de un resultado positivo a las autoridades competentes y, de conformidad con el artículo 9, apartado 1, a las UIP de otros Estados miembros. Cuando el resultado de un tratamiento automatizado, tras un examen individual por medios no automatizados, contemplado en el artículo 6, apartado 5, arroje un resultado negativo, este se podrá almacenar para evitar falsos resultados positivos mientras los datos de base no se hayan eliminado con arreglo al apartado 4 del presente artículo.

Artículo 13

Protección de los datos de carácter personal

1. Cada Estado miembro establecerá que, en lo que respecta al tratamiento de datos personales con arreglo a la presente Directiva, todo pasajero tendrá los mismos derechos de protección de sus datos personales, derechos de acceso, rectificación, supresión y restricción y derechos de indemnización y recurso judicial que los establecidos en el derecho de la Unión y nacional y en aplicación de los artículos 17, 18, 19 y 20 de la Decisión marco 2008/977/JAI. Se aplicarán, por lo tanto, dichos artículos.

2. Cada Estado miembro establecerá que las disposiciones adoptadas en el marco del derecho nacional en aplicación de los artículos 21 y 22 de la Decisión marco 2008/977/JAI sobre la confidencialidad del tratamiento y la seguridad de los datos se aplicarán también a todo tratamiento de datos personales con arreglo a la presente Directiva.

3. La presente Directiva se entenderá sin perjuicio de la aplicabilidad de la Directiva 95/46/CE del Parlamento Europeo y del Consejo ([1]) al tratamiento de datos personales por las compañías aéreas, en particular sus obligaciones de tomar las medidas técnicas y de organización adecuadas para proteger la seguridad y la confidencialidad de los datos personales.

4. Los Estados miembros prohibirán el tratamiento de datos PNR que revele el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud, la vida sexual o la orientación sexual de una persona. En el caso de que la UIP reciba datos PNR que revelen tal información, los suprimirá inmediatamente.

5. Los Estados miembros garantizarán que las UIP conserven la documentación relativa a todos los sistemas y procedimientos de tratamiento bajo su responsabilidad. Dicha documentación constará como mínimo de los siguientes elementos:

a) el nombre y los datos de contacto de la organización y del personal de la UIP encargados del tratamiento de los datos PNR y los distintos niveles de autorización de acceso;

b) las solicitudes cursadas por las autoridades competentes y por las UIP de otros Estados miembros;

c) todas las solicitudes y transmisiones de datos PNR a un tercer país.

La UIP pondrá toda la documentación a disposición de la autoridad nacional de control a petición de esta.

6. Los Estados miembros velarán por que la UIP lleve registros de, al menos, las operaciones de tratamiento siguientes: recogida, consulta, divulgación y supresión. Los registros de consulta y divulgación mostrarán, en particular, la finalidad, la fecha y la hora de tales operaciones y, en la medida de lo posible, la identidad de la persona que consultó o divulgó los datos PNR y la identidad de los receptores de dichos datos. Los registros se utilizarán exclusivamente a efectos de verificación, de autocontrol, de garantizar la integridad de los datos y su seguridad o de auditoría. La UIP pondrá los registros a disposición de la autoridad nacional de control a petición de esta.

Dichos registros se conservarán por un período de cinco años.

7. Los Estados miembros velarán por que sus UIP apliquen las medidas y los procedimientos técnicos y organizativos adecuados para garantizar el elevado nivel de seguridad correspondiente a los riesgos que entrañen el tratamiento y las características de los datos PNR.

8. Los Estados miembros garantizarán que, cuando sea probable que una violación de los datos personales dé lugar a un elevado riesgo para la protección de estos o afecte negativamente a la intimidad del interesado, la UIP comunique, sin demora injustificada, dicha violación al interesado y a la autoridad supervisora nacional.

Artículo 14

Sanciones

Los Estados miembros establecerán el régimen de sanciones aplicables a los incumplimientos de las disposiciones nacionales adoptadas en aplicación de la presente Directiva y adoptarán toda medida necesaria para garantizar la aplicación de estas.

En particular, los Estados miembros establecerán sanciones, incluidas las pecuniarias, contra las compañías aéreas que no transmitan datos con arreglo a lo establecido en el artículo 8, o no lo hagan en el formato exigido.

Dichas sanciones deberán ser efectivas, proporcionadas y disuasorias.

([1]) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

Artículo 15

Autoridad nacional de control

1. Cada Estado miembro dispondrá que la autoridad nacional de control a que se refiere el artículo 25 de la Decisión marco 2008/977/JAI sea responsable de asesorar sobre la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros de conformidad con la presente Directiva y de controlar dicha aplicación. Será aplicable el artículo 25 de la Decisión marco 2008/977/JAI.

2. Las autoridades nacionales de control realizarán las actividades a que se refiere el apartado 1 con el fin de proteger los derechos fundamentales relativos al tratamiento de los datos personales.

3. Cada autoridad nacional de control:

a) conocerá de las reclamaciones presentadas por cualquier interesado, investigará el asunto e informará al interesado de los progresos y el resultado de su reclamación en un plazo de tiempo razonable;

b) verificará la legalidad del tratamiento de los datos, realizará investigaciones, inspecciones y auditorías de conformidad con el derecho nacional, bien por propia iniciativa, bien sobre la base de la reclamación a que se refiere la letra a).

4. Cada autoridad nacional de control asesorará, previa solicitud, a cualquier interesado en el ejercicio de los derechos establecidos en las disposiciones adoptadas con arreglo a la presente Directiva.

CAPÍTULO III

Disposiciones de aplicación

Artículo 16

Protocolos comunes y formatos de datos admitidos

1. Todas las transmisiones de datos PNR por las compañías aéreas a las UIP a efectos de la presente Directiva se efectuarán por medios electrónicos que ofrezcan garantías suficientes en relación con las medidas de seguridad técnicas y las medidas organizativas que rigen el tratamiento de datos que se va a llevar a cabo. En caso de fallo técnico, los datos PNR podrán ser transmitidos por cualquier otro medio adecuado, siempre que se mantenga el mismo nivel de seguridad y que se cumpla íntegramente el derecho de la Unión en materia de protección de datos.

2. Un año después de la fecha de la primera adopción por la Comisión, de conformidad con el apartado 3, de los protocolos comunes y los formatos de datos admitidos, toda transmisión de datos PNR por las compañías aéreas a las UIP a efectos de la presente Directiva se efectuará electrónicamente utilizando métodos seguros de conformidad con dichos protocolos comunes. Tales protocolos serán comunes a todas las transmisiones para garantizar la seguridad de los datos PNR durante la transmisión. Los datos PNR serán transmitidos en un formato de datos admitido que garantice su legibilidad por todas las partes interesadas. Se exigirá a todas las compañías aéreas que seleccionen e indiquen a la UIP el protocolo común y el formato de datos que se proponen utilizar en sus transmisiones.

3. Se elaborará una lista de los protocolos comunes y los formatos de datos admitidos que, en caso necesario, la Comisión adaptará mediante actos de ejecución. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 17, apartado 2.

4. Será de aplicación el apartado 1 mientras no se disponga de los protocolos comunes aceptados y de los formatos de datos admitidos a que se refieren los apartados 2 y 3.

5. En el plazo de un año desde la fecha de adopción de los protocolos comunes y formatos de datos admitidos a que se hace referencia en el apartado 2, cada Estado miembro se asegurará de que se adopten las medidas técnicas necesarias para poder utilizar los protocolos comunes y formatos de datos.

Artículo 17

Procedimiento de comité

1. La Comisión estará asistida por un comité que será un comité con arreglo al Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, será de aplicación el artículo 5 del Reglamento (UE) n.º 182/2011.

Si el comité no emite un dictamen, la Comisión no adoptará el proyecto de acto de ejecución y se aplicará el artículo 5, apartado 4, párrafo tercero del Reglamento (UE) n.º 182/2011.

CAPÍTULO IV

Disposiciones finales

Artículo 18

Transposición

1. Los Estados miembros pondrán en vigor a más tardar el 25 de mayo de 2018 las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo dispuesto en la presente Directiva. Informarán inmediatamente a la Comisión del texto de dichas disposiciones.

Cuando los Estados miembros adopten dichas disposiciones, estas incluirán una referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

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

Artículo 19

Revisión

1. Atendiendo a la información que le faciliten los Estados miembros, incluida la información estadística a que se refiere el artículo 20, apartado 2, la Comisión, a más tardar el 25 de mayo de 2020, realizará una revisión de todos los elementos de la presente Directiva y presentará y someterá un informe al Parlamento Europeo y al Consejo.

2. Al realizar la revisión, la Comisión prestará especial atención:

a) al cumplimiento de las normas aplicables de protección de los datos personales;

b) a la necesidad y la proporcionalidad de la recogida y del tratamiento de datos PNR para cada uno de los fines establecidos en la presente Directiva;

c) a la duración del período de conservación de datos;

d) a la eficacia del intercambio de información entre los Estados miembros, y

e) a la calidad de las evaluaciones, también con respecto a la información estadística recopilada de conformidad con el artículo 20.

3. El informe a que se refiere el apartado 1, incluirá asimismo un estudio de la necesidad, la proporcionalidad y la eficacia de la inclusión en el ámbito de aplicación de la presente Directiva, de la recogida y transmisión obligatoria de los datos PNR relativos a todos o determinados vuelos interiores de la UE. La Comisión tendrá en cuenta la experiencia adquirida por los Estados miembros, en especial por aquellos que aplican la presente Directiva a los vuelos interiores de la UE, de conformidad con el artículo 2. El informe estudiará también la necesidad de incluir en el ámbito de aplicación de la presente Directiva a agentes económicos que no sean compañías aéreas, tales como agencias de viaje y operadores turísticos que prestan servicios relacionados con los viajes, como la reserva de vuelos.

4. La Comisión presentará, en su caso, a la luz de la revisión efectuada con arreglo al presente artículo, una propuesta legislativa al Parlamento Europeo y al Consejo con vistas a la modificación de la presente Directiva.

Artículo 20

Datos estadísticos

1. Los Estados miembros proporcionarán anualmente a la Comisión un conjunto de información estadística sobre los datos PNR comunicados a las UIP. Las estadísticas no contendrán datos personales.

2. Las estadísticas incluirán, como mínimo:

a) el número total de pasajeros cuyos datos PNR hayan sido recopilados e intercambiados;

b) el número de pasajeros identificados para un examen ulterior.

Artículo 21

Relación con otros instrumentos

1. Los Estados miembros podrán seguir aplicando los convenios bilaterales o multilaterales o los acuerdos que mantengan entre sí sobre el intercambio de información entre las autoridades competentes, que estén en vigor el 24 de mayo de 2016, siempre que dichos acuerdos o disposiciones sean compatibles con la presente Directiva.

2. La presente Directiva se entenderá sin perjuicio de la aplicabilidad de la Directiva 95/46/CE al tratamiento de datos personales por las compañías aéreas.

3. La presente Directiva se entiende sin perjuicio de las obligaciones y compromisos de los Estados miembros o de la Unión en virtud de convenios bilaterales o multilaterales con terceros países.

Artículo 22

Entrada en vigor

La presente Directiva entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Los destinatarios de la presente Directiva son los Estados miembros de conformidad con los Tratados.

Hecho en Bruselas, el 27 de abril de 2016.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*La Presidenta*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

ANEXO I

Datos del registro de nombres de los pasajeros recopilados por las compañías aéreas

1. Localizador de registro PNR
2. Fecha de reserva/emisión del billete
3. Fecha(s) fechas de viaje prevista(s)
4. Nombre(s) y apellido(s)
5. Dirección y datos de contacto (número de teléfono, dirección de correo electrónico)
6. Todos los datos de pago, incluida la dirección de facturación
7. Itinerario completo del viaje para el PNR específico
8. Información sobre viajeros asiduos
9. Agencia de viajes/operador de viajes
10. Situación de vuelo del pasajero: confirmaciones, facturación, no comparecencia o pasajeros de última hora sin reserva
11. Información PNR escindida/dividida
12. Observaciones generales (incluida toda la información disponible sobre menores de 18 años no acompañados, como nombre y sexo del menor, edad, idiomas que habla, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de salida y vínculo con el menor, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de llegada y vínculo con el menor, agente en el lugar de salida y de llegada)
13. Información sobre el billete, incluidos el número del billete, la fecha de emisión, los billetes solo de ida y la indicación de la tarifa de los billetes electrónicos (Automatic Ticket Fare Quote)
14. Datos del asiento, incluido el número
15. Información sobre códigos compartidos
16. Toda la información relativa al equipaje
17. Número de viajeros y otros nombres de viajeros que figuran en el PNR
18. Cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema API) (incluidos el tipo, número, país de emisión y fecha de expiración de cualquier documento de identidad, nacionalidad, apellidos, nombre, sexo, fecha de nacimiento, compañía aérea, número de vuelo, fecha de salida, fecha de llegada, aeropuerto de salida, aeropuerto de llegada, hora de salida y hora de llegada)
19. Todo el historial de cambios de los datos PNR indicados en los números 1 a 18.

ANEXO II

Lista de los delitos a que se refiere el artículo 3, punto 9

1. pertenencia a una organización delictiva
2. trata de seres humanos
3. explotación sexual de niños y pornografía infantil
4. tráfico ilícito de estupefacientes y sustancias psicotrópicas
5. tráfico ilícito de armas, municiones y explosivos
6. corrupción
7. fraude, incluido el que afecte a los intereses financieros de la Unión
8. blanqueo del producto del delito y falsificación de moneda, con inclusión del euro
9. delitos informáticos/ciberdelincuencia
10. delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas
11. ayuda a la entrada y residencia ilegales
12. homicidio voluntario, agresión con lesiones graves
13. tráfico ilícito de órganos y tejidos humanos
14. secuestro, detención ilegal y toma de rehenes
15. robo organizado y a mano armada
16. tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte
17. falsificación y violación de derechos de propiedad intelectual o industrial de mercancías
18. falsificación de documentos administrativos y tráfico de documentos administrativos falsos
19. tráfico ilícito de sustancias hormonales y otros factores de crecimiento
20. tráfico ilícito de materiales radiactivos o sustancias nucleares
21. violación
22. delitos incluidos en la jurisdicción de la Corte Penal Internacional
23. secuestro de aeronaves y buques
24. sabotaje
25. tráfico de vehículos robados
26. espionaje industrial.

ISSN 1977-0685 (edición electrónica)
ISSN 1725-2512 (edición papel)

Oficina de Publicaciones de la Unión Europea
2985 Luxemburgo
LUXEMBURGO

ES