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