REGLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 23 de octubre de 2018

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

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

Vista la propuesta de la Comisión Europea,

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

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

De conformidad con el procedimiento legislativo ordinario ([2]),

Considerando lo siguiente:

(1) La protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal (datos personales) 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. También el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales garantiza ese derecho.

(2) El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo ([3]) proporciona a las personas físicas unos derechos protegidos jurídicamente, especifica las obligaciones de los responsables del tratamiento dentro de las instituciones y los organismos de la Unión en materia de tratamiento de datos y crea una autoridad de control independiente, el Supervisor Europeo de Protección de Datos, responsable de la vigilancia de los tratamientos de datos personales efectuados por las instituciones y los organismos de la Unión. Sin embargo, no se aplica al tratamiento de datos personales en el ejercicio de una actividad de las instituciones y los organismos de la Unión no comprendida en el ámbito de aplicación del Derecho de la Unión.

(3) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([4]) y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo ([5]) fueron adoptados el 27 de abril de 2016. Mientras que el Reglamento establece normas generales para proteger a las personas físicas en lo que respecta al tratamiento de los datos personales y para facilitar la libre circulación de datos personales en la Unión, la Directiva establece normas específicas para proteger a las personas físicas en lo que respecta al tratamiento de los datos personales y para garantizar la libre circulación de datos personales en la Unión en el ámbito de la cooperación judicial en materia penal y en el de la cooperación policial.

(4) El Reglamento (UE) 2016/679 dispone que se adapte el Reglamento (CE) n.º 45/2001 a fin de garantizar un marco sólido y coherente en materia de protección de datos en la Unión y permitir que pueda aplicarse al mismo tiempo que el Reglamento (UE) 2016/679.

(5) Redunda en interés de un enfoque coherente de la protección de datos personales en la Unión y de la libre circulación de datos personales en la Unión, armonizar, en la medida de lo posible, las normas de protección de datos de las instituciones, órganos y organismos de la Unión con las adoptadas para el sector público en los Estados miembros. Cuando las disposiciones del presente Reglamento apliquen los mismos principios que las disposiciones

---

([1]) DO C 288 de 31.8.2017, p. 107.

([2]) Posición del Parlamento Europeo de 13 de septiembre de 2018 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 11 de octubre de 2018.

([3]) 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).

([4]) 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) (DO L 119 de 4.5.2016, p. 1).

([5]) 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 2008/977/JAI (DO L 119 de 4.5.2016, p. 89).

del Reglamento (UE) 2016/679, según la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia»), ambas deben interpretarse de manera homogénea, en particular porque debe entenderse que la estructura del presente Reglamento es equivalente a la del Reglamento (UE) 2016/679.

(6) Se debe proteger a las personas cuyos datos personales son tratados por las instituciones y organismos de la Unión en cualquier contexto, por ejemplo, porque estas personas estén empleadas por dichas instituciones y organismos. El presente Reglamento no se aplica al tratamiento de datos personales de personas fallecidas. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y, en particular, a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

(7) A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas.

(8) El presente Reglamento se aplica al tratamiento de datos personales por parte de todas las instituciones, órganos y organismos de la Unión. 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. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento.

(9) En la Declaración n.º 21 relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, anexa al acta final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa, la Conferencia reconoció que podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 del TFUE, en razón de la naturaleza específica de dichos ámbitos. Por ello, debe dedicarse un capítulo específico del presente Reglamento de normas generales al tratamiento de datos personales de carácter operativo (datos personales operativos), tales como los datos personales que, en el marco de investigaciones de infracciones, sean tratados por órganos u organismos de la Unión cuando lleven a cabo actividades en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.

(10) La Directiva (UE) 2016/680 establece normas armonizadas para la protección y libre circulación de los datos personales tratados con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención. A fin de garantizar el mismo nivel de protección de las personas físicas mediante derechos protegidos jurídicamente en toda la Unión y evitar divergencias que dificulten el intercambio de datos personales entre los órganos u organismos de la Unión cuando lleven a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE y las autoridades competentes, las normas para la protección y la libre circulación de los datos personales operativos tratados por dichos órganos u organismos de la Unión deben ser coherentes con la Directiva (UE) 2016/680.

(11) Las normas generales del capítulo del presente Reglamento sobre el tratamiento de datos personales operativos deben aplicarse sin perjuicio de las normas especiales aplicables al tratamiento de datos personales operativos por parte de los órganos y organismos de la Unión cuando lleven a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE. Dichas normas especiales deben considerarse como *lex specialis* en relación con las disposiciones del capítulo del presente Reglamento relativo al tratamiento de datos personales operativos (*lex specialis derogat legi generali*). A fin de reducir la fragmentación jurídica, las normas especiales en materia de protección de datos aplicables al tratamiento de datos personales operativos por parte de los órganos y organismos de la Unión cuando lleven a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE deben ser coherentes con los principios en que se basa el capítulo del presente Reglamento sobre el tratamiento de datos personales operativos y con las disposiciones del presente Reglamento relativas a la supervisión independiente, los recursos, la responsabilidad y las sanciones.

(12) El capítulo del presente Reglamento sobre el tratamiento de datos personales operativos debe aplicarse a los órganos y organismos de la Unión cuando lleven a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE, si ejercen tales actividades ya sea como tarea principal o accesoria, con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales. No obstante, no debe aplicarse a Europol ni a la Fiscalía Europea hasta que se modifiquen los actos jurídicos que los establecen, a fin de que les sea aplicable, con sus adaptaciones, el capítulo del presente Reglamento sobre el tratamiento de datos personales operativos.

(13) La Comisión debe llevar a cabo una revisión del presente Reglamento, en especial del capítulo sobre el tratamiento de datos personales operativos. Asimismo, la Comisión debe revisar otros actos jurídicos adoptados sobre la base de los Tratados que regulen el tratamiento de datos personales operativos por los órganos y organismos de la Unión

cuando llevan a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE. Tras dicha revisión, a fin de garantizar la protección uniforme y coherente de las personas físicas en lo que respecta al tratamiento de los datos personales, la Comisión debe poder presentar las propuestas legislativas oportunas, en especial las adaptaciones que sean necesarias del capítulo del presente Reglamento sobre el tratamiento de datos personales operativos, a efectos de su aplicación a Europol y a la Fiscalía Europea,. Las adaptaciones deben tener en cuenta las disposiciones relativas a la supervisión independiente, los recursos, la responsabilidad y las sanciones.

(14) El presente Reglamento debe incluir en su ámbito de aplicación el tratamiento de datos personales de carácter administrativo, por ejemplo los datos relativos al personal, por los órganos u organismos de la Unión que lleven a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE.

(15) El presente Reglamento debe incluir en su ámbito de aplicación el tratamiento de datos personales por parte de las instituciones, órganos y organismos de la Unión que lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de la Unión Europea (TUE). El presente Reglamento no debe incluir en su ámbito de aplicación el tratamiento de datos personales por parte de las misiones mencionadas en el artículo 42, apartado 1, y en los artículos 43 y 44 del TUE, que aplican la política común de seguridad y defensa. En su caso, se presentarán propuestas pertinentes para regular más el tratamiento de datos personales en el ámbito de la política común de seguridad y defensa.

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

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

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

(19) El consentimiento debe prestarse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos personales que le conciernen, como una declaración por escrito, también por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe prestarse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe prestarse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de prestar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta. Al mismo tiempo, el interesado debe tener derecho a revocar su consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su revocación. Para garantizar que el consentimiento se haya prestado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos personales en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento y sea por lo tanto improbable que el consentimiento se hubiese prestado libremente

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

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

(21) De conformidad con el principio de responsabilidad proactiva, cuando las instituciones y organismos de la Unión transmitan datos personales en el seno de la misma institución u organismo de la Unión y el destinatario no forme parte del responsable del tratamiento, o los transmitan a otras instituciones u organismos de la Unión, deben verificar si dichos datos personales son necesarios para el ejercicio legítimo de las funciones comprendidas en el ámbito de competencias del destinatario. En particular, tras la petición de transmisión de datos personales por parte de un destinatario, el responsable debe verificar la existencia de un motivo pertinente para el tratamiento lícito de los datos personales por su parte así como la competencia del destinatario. El responsable también debe efectuar una evaluación provisional de la necesidad de la transmisión de dichos datos. En caso de albergar dudas sobre tal necesidad, el responsable del tratamiento debe pedir al destinatario que aporte información complementaria. El destinatario debe garantizar la posibilidad de verificar posteriormente la necesidad de la transmisión de los datos.

(22) Para que el tratamiento sea lícito, los datos personales deben ser tratados sobre la base de la necesidad del desempeño de una función realizada en interés público por parte de las instituciones y organismos de la Unión o en el ejercicio de sus potestades públicas, la necesidad de cumplir una obligación legal del responsable del tratamiento o sobre alguna otra base legítima con arreglo al presente Reglamento, incluido el consentimiento del interesado, la necesidad para el cumplimiento de un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato. El tratamiento de datos personales efectuado a cargo de las instituciones y organismos de la Unión para el desempeño de funciones de interés público incluye el tratamiento de datos personales necesarios para la gestión y el funcionamiento de dichas instituciones y organismos. El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

(23) La normativa de la Unión a la que se refiere el presente Reglamento debe ser clara y precisa y su aplicación previsible para quienes estén sujetos a ella, de conformidad con los requisitos establecidos en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

(24) Las normas internas a las que se refiere el presente Reglamento deben constituir actos de aplicación general claros y precisos destinados a producir efectos jurídicos frente a los interesados. Deben adoptarse al nivel de gestión más elevado de las instituciones y organismos de la Unión, dentro de sus competencias y respecto de materias relacionadas con su funcionamiento. Deben publicarse en el *Diario Oficial de la Unión Europea*. La aplicación de dichas normas debe ser previsible para quienes estén sujetos a ellas, de conformidad con lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Las normas internas pueden adoptar la forma de decisiones, en particular cuando sean adoptadas por instituciones de la Unión.

(25) El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si el tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de potestades públicas conferidas al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas: cualquier relación entre estos fines y los fines del tratamiento ulterior previsto; el contexto en el que se recogieron los datos, en particular, las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior; la naturaleza de los datos personales; las consecuencias para los interesados del tratamiento ulterior previsto; y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

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

(27) Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse, en particular, a la elaboración de perfiles de personalidad y a la obtención de datos personales relativos a niños cuando se ofrezcan servicios directamente a un niño en los sitios web de las instituciones y organismos de la Unión, tales como los servicios de comunicación interpersonal o la venta por internet de entradas, y el tratamiento de los datos personales se base en el consentimiento.

(28) Cuando los destinatarios establecidos en la Unión distintos de las instituciones y organismos de la Unión quieran que las instituciones y organismos de la Unión les transmitan datos personales, dichos destinatarios deben demostrar que la transmisión es necesaria para el ejercicio de sus funciones llevadas a cabo en interés público o bien para el ejercicio de las potestades públicas que tienen conferidas. Alternativamente, dichos destinatarios deberán demostrar que la transmisión es necesaria para una finalidad específica de interés público y el responsable del tratamiento debe determinar si existe alguna razón que permita suponer que se perjudicarán los intereses legítimos del interesado. En tales casos, el responsable del tratamiento debe ponderar de manera demostrable los diferentes intereses a fin de calcular la proporcionalidad de la transmisión de datos personales solicitada. Esa finalidad específica de interés

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

público puede guardar relación con la transparencia de las instituciones y organismos de la Unión. Además, las instituciones y organismos de la Unión deben demostrar esta necesidad en el momento en que ellos mismos inicien la transmisión, con arreglo al principio de transparencia y buena administración. Debe entenderse que los requisitos establecidos en el presente Reglamento para las transmisiones a destinatarios establecidos en la Unión distintos de las instituciones y organismos de la Unión son complementarios a las condiciones para un tratamiento lícito.

(29) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Tales datos personales no deben ser objeto de tratamiento, salvo que se cumplan las condiciones específicas definidas en el presente Reglamento. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Además de los requisitos específicos para el tratamiento de datos sensibles, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado preste su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

(30) Las categorías especiales de datos personales que merecen mayor protección deben tratarse con fines relacionados con la salud únicamente cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas de asistencia social y sanitaria. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional. El Derecho de la Unión debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas.

(31) El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse según se define en el Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo ([1]), es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que se traten los datos personales con otros fines.

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

(33) El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y las libertades del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos. El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines

([1]) Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo (DO L 354 de 31.12.2008, p. 70).

estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos). Las instituciones y organismos de la Unión deben establecer garantías adecuadas para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos en el Derecho de la Unión, garantías que pueden incluir normas internas adoptadas por las instituciones y organismos de la Unión en cuestiones relacionadas con su funcionamiento.

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

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

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

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

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

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

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

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

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

(42) En los casos en que los datos personales puedan ser tratados lícitamente porque el tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de potestades públicas conferidas al responsable del tratamiento, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y las libertades fundamentales del interesado.

(43) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento automatizado de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación

económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor. A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y el contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado e impedir, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o tratamiento que dé lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas.

(44) Los actos jurídicos adoptados con arreglo a los Tratados o las normas internas adoptadas por las instituciones y organismos de la Unión en cuestiones relacionadas con su funcionamiento pueden imponer limitaciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, a la confidencialidad de las comunicaciones electrónicas así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública y para la prevención, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales. Se incluye en lo anterior la protección frente a las amenazas contra la seguridad pública, la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la seguridad interna de las instituciones y organismos de la Unión, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular los objetivos de la política exterior y de seguridad común de la Unión o un importante interés económico o financiero de la Unión o de un Estado miembro, y el mantenimiento de registros públicos por razones de interés público general o la protección del interesado o de los derechos y libertades de terceros, incluida la protección social, la salud pública y los fines humanitarios.

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

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

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

(48) La protección de los derechos y las libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con este, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan, en particular, los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

(49) El Reglamento (UE) 2016/679 establece que los responsables del tratamiento de datos demuestren el cumplimiento mediante la adhesión a mecanismos de certificación aprobados. Del mismo modo, las instituciones y organismos de la Unión deben poder demostrar el cumplimiento de lo dispuesto en el presente Reglamento mediante la obtención de una certificación de conformidad con el artículo 42 del Reglamento (UE) 2016/679.

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

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

(52) Para demostrar la conformidad con el presente Reglamento, los responsables del tratamiento deben mantener registros de las actividades de tratamiento bajo su responsabilidad y los encargados del tratamiento deben mantener registros de las categorías de actividades de tratamiento bajo su responsabilidad. Las instituciones y organismos de la Unión están obligados a cooperar con el Supervisor Europeo de Protección de Datos y a poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento. Salvo que no sea adecuado habida cuenta del tamaño de una institución u organismo de la Unión, las instituciones y organismos de la Unión deben tener la posibilidad de establecer un archivo central de información de sus actividades de tratamiento. Por razones de transparencia, deben tener la posibilidad de hacerlo público.

(53) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los

datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

(54) Las instituciones y organismos de la Unión deben garantizar la confidencialidad de las comunicaciones electrónicas con arreglo al artículo 7 de la Carta. En particular, las instituciones y organismos de la Unión deben garantizar la seguridad de sus redes de comunicación electrónica. Deben proteger la información relativa a los equipos terminales de los usuarios que acceden a los contenidos públicos de sus sitios web y a sus aplicaciones para móviles disponibles al público, de conformidad con la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([1]). También deben proteger los datos personales almacenados en las guías de usuarios.

(55) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales podrían entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar dicha violación de la seguridad de los datos personales al Supervisor Europeo de Protección de Datos, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida. Si dicha dilación está justificada, se debe dar a conocer, tan pronto como sea posible, información menos sensible o menos específica acerca de la violación, en lugar de solucionar totalmente el incidente subyacente antes de notificarlo.

(56) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que pueda entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con el Supervisor Europeo de Protección de Datos, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales.

(57) El Reglamento (CE) n.º 45/2001 establece la obligación general del responsable del tratamiento de notificar el tratamiento de datos personales al delegado de protección de datos. Salvo que no sea adecuado habida cuenta del tamaño de la institución u organismo de la Unión, el delegado de protección de datos debe mantener un registro de las operaciones de tratamiento que se le notifiquen. Además de esta obligación general, deben establecerse procedimientos y mecanismos eficaces para efectuar un seguimiento de las operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos procedimientos deben establecerse también, en particular, cuando los tipos de operaciones de tratamiento impliquen el uso de nuevas tecnologías o sean de una nueva clase en relación con la cual el responsable del tratamiento no haya realizado previamente una evaluación de impacto relativa a la protección de datos o si resultan necesarias habida cuenta del tiempo transcurrido desde el tratamiento inicial. En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la gravedad y probabilidad concretas del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento.

(58) Debe consultarse al Supervisor Europeo de Protección de Datos antes de iniciar las actividades de tratamiento si una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas y mecanismos de seguridad destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse con medidas razonables en términos de tecnología disponible y costes de aplicación. Existe la probabilidad de que ese alto riesgo se deba a determinados tipos de tratamiento y al alcance y frecuencia de este, lo que también podría ocasionar daños y perjuicios o una injerencia en los derechos y libertades de la persona física. El Supervisor Europeo de Protección de Datos debe responder a la solicitud de consulta dentro de un plazo determinado. Sin embargo, la

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

ausencia de respuesta del Supervisor Europeo de Protección de Datos dentro de dicho plazo no debe obstar a cualquier intervención de dicho Supervisor basada en las funciones y potestades que le atribuye el presente Reglamento, incluido el poder de prohibir operaciones de tratamiento. Como parte de dicho proceso de consulta, debería poder presentarse al Supervisor Europeo de Protección de Datos el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y las libertades de las personas físicas.

(59) El Supervisor Europeo de Protección de Datos debe ser informado acerca de las medidas administrativas y consultado sobre las normas internas adoptadas por las instituciones y organismos de la Unión en cuestiones relacionadas con el funcionamiento de estos cuando dispongan el tratamiento de datos personales, establezcan condiciones para limitar los derechos de los interesados u ofrezcan garantías para los derechos de este, a fin de garantizar que el tratamiento previsto sea conforme con el presente Reglamento, en particular, en lo relativo a mitigar los riesgos que implique para el interesado.

(60) El Reglamento (UE) 2016/679 estableció el Comité Europeo de Protección de Datos como organismo independiente de la Unión dotado de personalidad jurídica. El Comité debe contribuir a la aplicación coherente del Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 en toda la Unión, entre otras cosas, asesorando a la Comisión. Al mismo tiempo, el Supervisor Europeo de Protección de Datos seguirá ejerciendo sus funciones supervisoras y consultivas respecto a todas las instituciones y organismos de la Unión, por iniciativa propia o a petición. A fin de garantizar la coherencia de las normas de protección de datos en toda la Unión, al elaborar propuestas o recomendaciones, la Comisión debe esforzarse por consultar con el Supervisor Europeo de Protección de Datos. La Comisión debe llevar a cabo consultas de manera obligatoria tras la adopción de actos legislativos o durante la preparación de actos delegados y actos de ejecución, tal como se define en los artículos 289, 290 y 291 del TFUE, y tras la adopción de recomendaciones y propuestas relativas a acuerdos con terceros países y organizaciones internacionales, con arreglo al artículo 218 del TFUE que repercutan en el derecho a la protección de los datos personales. En estos casos, la Comisión debe estar obligada a consultar al Supervisor Europeo de Protección de Datos, excepto cuando el Reglamento (UE) 2016/679 prevea una consulta obligatoria del Comité Europeo de Protección de Datos, por ejemplo, sobre decisiones de adecuación o actos delegados relativos a iconos normalizados y requisitos para los mecanismos de certificación. Cuando dicho acto sea de especial importancia para la protección de los derechos y libertades de las personas físicas en relación con el tratamiento de datos personales, la Comisión debe tener la posibilidad de consultar, además, al Comité Europeo de Protección de Datos. En estos casos, el Supervisor Europeo de Protección de Datos debe, como miembro del Comité Europeo de Protección de Datos, coordinar su trabajo con este último a fin de emitir un dictamen conjunto. El Supervisor Europeo de Protección de Datos y, si procede, el Comité Europeo de Protección de Datos deben ofrecer su asesoramiento escrito en un plazo de ocho semanas. El plazo debe ser más corto en casos de urgencia o cuando se considere conveniente por otro motivo, por ejemplo, cuando la Comisión esté preparando actos delegados y de ejecución.

(61) De conformidad con el artículo 75 del Reglamento (UE) 2016/679, el Supervisor Europeo de Protección de Datos debe hacerse cargo de la secretaría del Comité Europeo de Protección de Datos.

(62) En todas las instituciones y organismos de la Unión, el delegado de protección de datos debe velar por que se aplique lo dispuesto en el presente Reglamento y asesorar a los responsables y encargados del tratamiento en el ejercicio de sus obligaciones. El delegado debe ser una persona con conocimientos especializados de la normativa y práctica en materia de protección de datos, que se deben determinar, en particular, en función de las operaciones de tratamiento de datos que lleven a cabo el responsable o el encargado y de la protección exigida para los datos personales tratados. Los delegados de protección de datos deben estar en condiciones de desempeñar sus funciones y tareas con independencia.

(63) Si los datos personales se transfieren de las instituciones y organismos de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, debe respetarse el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento. Se deben aplicar las mismas garantías en caso de transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento y respetando los derechos y las libertades fundamentales establecidos en la Carta. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.

(64) La Comisión puede decidir, con arreglo al artículo 45 del Reglamento (UE) 2016/679 o al artículo 36 de la Directiva (UE) 2016/680, que un tercer país, un territorio o sector específico en un tercer país o una organización internacional ofrece un nivel de protección de datos adecuado. En estos casos, las instituciones y organismos de la Unión pueden realizar transferencias de datos personales a estos países u organizaciones internacionales sin que se requiera obtener otro tipo de autorización.

(65) En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a cláusulas tipo de protección de datos adoptadas por la Comisión o por el Supervisor Europeo de Protección de Datos, o a cláusulas contractuales autorizadas por este último. Cuando el encargado del tratamiento no es una institución u organismo de la Unión, dichas garantías adecuadas pueden consistir en normas corporativas vinculantes, códigos de conducta y mecanismos de certificación utilizados para realizar transferencias internacionales de conformidad con el Reglamento (UE) 2016/679. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto. Las transferencias también pueden realizarlas instituciones y organismos de la Unión a entidades o autoridades públicas de terceros países o a organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes se debe recabar la autorización del Supervisor Europeo de Protección de Datos.

(66) La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o el Supervisor Europeo de Protección de Datos no debe obstar a que los responsables o encargados incluyan las cláusulas tipo de protección de datos en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por el Supervisor Europeo de Protección de Datos, ni mermen los derechos o las libertades fundamentales de los interesados. Se debe alentar a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos.

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

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

(69) Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre las instituciones y organismos de la Unión y autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, autoridades de supervisión financiera y servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso de contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el

dopaje en el deporte. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de prestar su consentimiento. En ausencia de una decisión de adecuación, el Derecho de la Unión puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional. Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para prestar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados.

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

(71) Cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información. Al mismo tiempo, es posible que las autoridades de control nacionales y el Supervisor Europeo de Protección de Datos se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de su jurisdicción. Sus esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por potestades preventivas o correctivas insuficientes, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. Por consiguiente, es necesario fomentar una cooperación más estrecha entre el Supervisor Europeo de Protección de Datos y las autoridades de control nacionales para contribuir al intercambio de información con sus homólogos internacionales.

(72) El establecimiento del Supervisor Europeo de Protección de Datos en el Reglamento (CE) n.º 45/2001, al que se ha facultado para desempeñar sus funciones y ejercer sus competencias con plena independencia, constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos personales. El presente Reglamento debe reforzar y aclarar aún más su función e independencia. El Supervisor Europeo de Protección de Datos será una persona cuya independencia esté fuera de toda duda y que posea una experiencia y competencia notorias para el desempeño de las funciones de Supervisor Europeo de Protección de Datos, como pertenecer o haber pertenecido a una de las autoridades de control establecidas con arreglo al artículo 51 del Reglamento (UE) 2016/679.

(73) Para garantizar la supervisión y ejecución coherentes de las normas de protección de datos en toda la Unión, el Supervisor Europeo de Protección de Datos debe tener las mismas funciones y potestades efectivas que las autoridades de control nacionales, incluidas potestades de investigación, potestades correctivas y de sanción y potestades de autorización y de consulta, especialmente en casos de reclamaciones de personas físicas, facultad para poner en conocimiento del Tribunal de Justicia las infracciones del presente Reglamento y capacidad para ejercitar acciones judiciales conforme a las disposiciones de Derecho primario. Dichas potestades deben incluir también la de imponer una limitación temporal o definitiva al tratamiento, incluida su prohibición. Para evitar costes superfluos y molestias excesivas para las personas afectadas, toda medida del Supervisor Europeo de Protección de Datos debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, debe tener en cuenta las circunstancias de cada caso concreto y respetar el derecho de todas las personas a ser oídas antes de que se adopte cualquier medida. Toda medida jurídicamente vinculante del Supervisor Europeo de Protección de Datos debe constar por escrito, ser clara e inequívoca, indicar la fecha en que se dictó, llevar la firma del Supervisor Europeo de Protección de Datos, especificar los motivos de la misma y mencionar el derecho a la tutela judicial efectiva.

(74) A fin de preservar la independencia del Tribunal de Justicia en el desempeño de sus funciones judiciales, incluida la toma de decisiones, la competencia en materia de supervisión del Supervisor Europeo de Protección de Datos no debe abarcar el tratamiento de datos personales por parte del Tribunal de Justicia cuando actúe en ejercicio de su función judicial. Para dichas operaciones de tratamiento, el Tribunal de Justicia debe establecer una supervisión independiente, de conformidad con el artículo 8, apartado 3, de la Carta, por ejemplo a través de un mecanismo interno.

(75) Las decisiones del Supervisor Europeo de Protección de Datos relacionadas con excepciones, garantías, autorizaciones y condiciones relativas a los tratamientos de datos, según se definen en el presente Reglamento, serán publicadas en el informe de actividad. Con independencia de la publicación anual del informe de actividad, el Supervisor Europeo de Protección de Datos podrá publicar informes sobre temas específicos.

(76) El Supervisor Europeo de Protección de Datos deberá cumplir lo dispuesto en el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo ([1]).

(77) A fin de proteger a las personas físicas con respecto al tratamiento de sus datos personales y de facilitar la libre circulación de los datos personales en el mercado interior, las autoridades de control nacionales supervisan la aplicación del Reglamento (UE) 2016/679 y contribuyen a que esta sea coherente en toda la Unión. Para aumentar la coherencia en la aplicación de las normas de protección de datos aplicables en los Estados miembros y de las aplicables a las instituciones y organismos de la Unión, el Supervisor Europeo de Protección de Datos debe cooperar de manera efectiva con las autoridades de control nacionales.

(78) En algunos casos, el Derecho de la Unión prevé un modelo de supervisión coordinada, compartido por el Supervisor Europeo de Protección de Datos y las autoridades de control nacionales. El Supervisor Europeo de Protección de Datos es además la autoridad de control de Europol y, a esos fines, se ha establecido un modelo específico de cooperación con las autoridades de control nacionales mediante un consejo de cooperación con funciones consultivas. Para mejorar la supervisión efectiva y el cumplimiento de las normas sustantivas de protección de datos, debe introducirse en la Unión un modelo único y coherente de supervisión coordinada. Por ello, la Comisión debe presentar, en su caso, propuestas legislativas para modificar actos jurídicos de la Unión que establezcan un modelo de supervisión coordinada, a fin de armonizarlos con el modelo de supervisión coordinada del presente Reglamento. El Comité Europeo de Protección de Datos debe servir de foro único para garantizar una supervisión eficaz y coordinada en todos los ámbitos.

(79) Todo interesado debe tener derecho a presentar una reclamación ante el Supervisor Europeo de Protección de Datos, y derecho a la tutela judicial efectiva ante el Tribunal de Justicia de conformidad con los Tratados, si considera que se vulneran sus derechos con arreglo al presente Reglamento o en caso de que el Supervisor Europeo de Protección de Datos no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado. La investigación abierta a raíz de una queja debe llevarse a cabo, bajo control judicial, en la medida en que sea adecuada en el caso específico. El Supervisor Europeo de Protección de Datos debe informar al interesado de la evolución y el resultado de la reclamación en un plazo razonable. Si el asunto requiere una mayor coordinación con una autoridad de control nacional, se debe facilitar información intermedia al interesado. Para facilitar la presentación de reclamaciones, el Supervisor Europeo de Protección de Datos debe adoptar medidas como el suministro de un formulario de reclamaciones, que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

(80) Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento debe tener derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos, con arreglo a las condiciones previstas en los Tratados.

(81) Para fortalecer la función supervisora del Supervisor Europeo de Protección de Datos y la aplicación eficaz del presente Reglamento, el primero debe estar facultado para imponer multas administrativas, como sanción de último recurso. Las multas deben aspirar a sancionar a las instituciones u organismos de la Unión, más que a los individuos, que incumplan el presente Reglamento, impedir futuras violaciones del mismo y fomentar una cultura de protección de los datos personales dentro de las instituciones y organismos de la Unión. El presente Reglamento debe indicar las infracciones objeto de multas administrativas, así como los límites máximos y los criterios para fijar las correspondientes multas. El Supervisor Europeo de Protección de Datos debe determinar la cuantía de la multa en cada caso individual, teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo a la naturaleza, gravedad y duración de la infracción, sus consecuencias y las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o mitigar las consecuencias de la infracción. Al imponer una multa administrativa a una institución u organismo de la Unión, el Supervisor Europeo de Protección de Datos debe considerar la proporcionalidad de su cuantía. El procedimiento administrativo para la imposición de multas a instituciones y organismos de la Unión debe respetar los principios generales del Derecho de esta, según la interpretación del Tribunal de Justicia.

(82) El interesado que considere vulnerados los derechos reconocidos por el presente Reglamento debe tener derecho a conferir mandato a una entidad, organización o asociación sin ánimo de lucro que esté constituida con arreglo al Derecho de la Unión o de un Estado miembro, tenga objetivos legales que sean de interés público y actúe en el

([1]) Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

ámbito de la protección de los datos personales, para que presente en su nombre una reclamación ante el Supervisor Europeo de Protección de Datos. Dicha entidad, organización o asociación debe tener la posibilidad de ejercer el derecho a la tutela judicial en nombre de los interesados o el derecho a recibir una indemnización en nombre de estos.

(83) El incumplimiento por parte de un funcionario u otro agente de la Unión de las obligaciones del presente Reglamento dará lugar a la apertura de un expediente disciplinario u otro tipo de acción, de conformidad con las disposiciones fijadas en el Estatuto de los funcionarios de la Unión Europea o en el régimen aplicable a los otros agentes de la Unión, establecido en el Reglamento (CEE, Euratom, CECA) n.º 259/68 del Consejo ([1]) (en lo sucesivo, «Estatuto de los funcionarios»).

(84) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([2]). El procedimiento de examen debe seguirse para la adopción de cláusulas contractuales tipo entre responsables del tratamiento y encargados del tratamiento y entre encargados del tratamiento, para la adopción de una lista de operaciones de tratamiento que exigen la consulta previa del Supervisor Europeo de Protección de Datos por parte de los responsables del tratamiento de los datos personales para el cumplimiento de una función realizada en interés público, y para la adopción de cláusulas contractuales tipo que ofrezcan unas garantías adecuadas para las transferencias internacionales.

(85) Debe protegerse la información confidencial que las autoridades estadísticas de la Unión y nacionales recojan para la elaboración de las estadísticas oficiales europeas y nacionales. Las estadísticas europeas deben desarrollarse, elaborarse y difundirse con arreglo a los principios estadísticos enunciados en el artículo 338, apartado 2, del TFUE. El Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo ([3]) facilita especificaciones adicionales sobre la confidencialidad estadística aplicada a las estadísticas europeas.

(86) Procede derogar el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE del Parlamento Europeo, del Consejo y de la Comisión ([4]). Las referencias al Reglamento y a la Decisión derogados deben entenderse hechas al presente Reglamento.

(87) Para garantizar la independencia plena de los miembros de la autoridad de control independiente, el mandato del actual Supervisor Europeo de Protección de Datos y del actual Supervisor Adjunto no debe verse afectado por el presente Reglamento. El actual Supervisor Adjunto debe permanecer en su puesto hasta el final de su mandato, a menos que se dé alguna de las condiciones para la finalización prematura del mandato del Supervisor Europeo de Protección de Datos establecidas en el presente Reglamento. Las disposiciones pertinentes del presente Reglamento deben aplicarse al Supervisor Adjunto hasta el final de su mandato.

(88) De acuerdo con el principio de proporcionalidad, es necesario y conveniente para alcanzar el objetivo fundamental de garantizar un nivel equivalente de protección de las personas físicas por lo que respecta al tratamiento de datos personales y la libre circulación de datos personales en la Unión establecer normas sobre el tratamiento de datos personales en las instituciones y organismos de la Unión. El presente Reglamento no excede de lo necesario para alcanzar los objetivos perseguidos, de conformidad con lo dispuesto en el artículo 5, apartado 4, del TUE.

(89) El Supervisor Europeo de Protección de Datos fue consultado de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001 y emitió su dictamen el 15 de marzo de 2017 ([5]).

([1]) DO L 56 de 4.3.1968, p. 1.

([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).

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

([4]) Decisión n.º 1247/2002/CE del Parlamento Europeo, del Consejo y de la Comisión, de 1 de julio de 2002, relativa al estatuto y a las condiciones generales de ejercicio de las funciones de Supervisor Europeo de Protección de Datos (DO L 183 de 12.7.2002, p. 1).

([5]) DO C 164 de 24.5.2017, p. 2.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y objetivos

1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por las instituciones y organismos de la Unión y las normas relativas a la libre circulación de dichos datos entre ellos o entre ellos y destinatarios establecidos en la Unión.

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

3. El Supervisor Europeo de Protección de Datos supervisará la aplicación de las disposiciones del presente Reglamento a todas las operaciones de tratamiento realizadas por las instituciones y organismos de la Unión.

Artículo 2

Ámbito de aplicación

1. El presente Reglamento se aplica al tratamiento de datos personales por parte de todas las instituciones y organismos de la Unión.

2. Solo el artículo 3 y el capítulo IX del presente Reglamento serán aplicables al tratamiento de datos personales operativos por los órganos y organismos de la Unión cuando lleven a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE.

3. El presente Reglamento no se aplicará al tratamiento de datos personales operativos por parte de Europol y de la Fiscalía Europea hasta que el Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo ([1]), y el Reglamento (UE) 2017/1939 del Consejo ([2]) se adapten con arreglo al artículo 98 del presente Reglamento.

4. El presente Reglamento no se aplicará al tratamiento de datos personales por parte de las misiones mencionadas en el artículo 42, apartado 1, y en los artículos 43 y 44 del TUE.

5. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

Artículo 3

Definiciones

A efectos del presente Reglamento, se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable (en lo sucesivo, «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) «datos personales operativos»: todos los datos personales tratados por los órganos u organismos de la Unión cuando lleven a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE a fin de realizar los objetivos y funciones establecidos en los actos jurídicos por los que se crean dichos órganos u organismos;

([1]) Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO L 135 de 24.5.2016, p. 53).

([2]) Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea (DO L 283 de 31.10.2017, p. 1).

3) «tratamiento»: cualquier operación o conjunto de operaciones realizadas en 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;

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

5) «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;

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

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

8) «responsable del tratamiento» o «responsable»: la institución o el organismo o la dirección general u otra entidad organizativa de la Unión que, por sí sola o conjuntamente con otros, determine los fines y medios del tratamiento de datos personales; cuando los fines y medios de ese tratamiento se determinen en un acto específico de la Unión, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser establecidos por el Derecho de la Unión;

9) «responsables del tratamiento distintos de las instituciones y organismos de la Unión»: los responsables del tratamiento en el sentido del artículo 4, punto 7, del Reglamento (UE) 2016/679 y los responsables del tratamiento en el sentido del artículo 3, punto 8, de la Directiva (UE) 2016/680;

10) «instituciones y organismos de la Unión»: las instituciones, los órganos y los organismos de la Unión establecidos por el TUE, el TFUE o el Tratado Euratom o sobre la base de cualquiera de ellos;

11) «autoridad competente»: cualquier autoridad pública de un Estado miembro 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;

12) «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;

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

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

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

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

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

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

19) «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;

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

21) «organización internacional»: una organización 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;

22) «autoridad de control nacional»: una autoridad pública independiente establecida por un Estado miembro con arreglo al artículo 51 del Reglamento (UE) 2016/679 o al artículo 41 de la Directiva (UE) 2016/680;

23) «usuario»: cualquier persona física que use una red o un equipo terminal que funcionen bajo el control de las instituciones y organismos de la Unión;

24) «guía»: guía de usuarios disponible para el público o guía interna de usuarios disponible dentro de las instituciones y organismos de la Unión o compartida entre estos, ya sea en formato impreso o electrónico;

25) «red de comunicaciones electrónicas»: un sistema de transmisión, basado o no en una infraestructura permanente o en una capacidad de administración centralizada, y, cuando proceda, los equipos de conmutación o enrutamiento y otros recursos, incluidos los elementos de red que no son activos, que permitan la transmisión de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, las redes terrestres fijas (de conmutación de circuitos y de paquetes, incluida internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transmitida;

26) «equipo terminal»: un equipo terminal tal como se define en el artículo 1, punto 1, de la Directiva 2008/63/CE de la Comisión ([2]).

CAPÍTULO II

PRINCIPIOS GENERALES

Artículo 4

Principios relativos al tratamiento de datos personales

1. Los datos personales serán:

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

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 13, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

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

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

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

([2]) Directiva 2008/63/CE de la Comisión, de 20 de junio de 2008, relativa a la competencia de los mercados de equipos terminales de telecomunicaciones (DO L 162 de 21.6.2008, p. 20).

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 13, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

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

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

Artículo 5

Licitud del tratamiento

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

a) el tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de potestades públicas conferidas a las instituciones y organismos de la Unión;

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

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

d) el interesado ha prestado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

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

2. La base del tratamiento indicado en el apartado 1, letras a) y b), se establecerá en el Derecho de la Unión.

Artículo 6

Tratamiento para otro fin compatible

Cuando el tratamiento para un fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en una norma de la Unión que constituya una medida necesaria y proporcionada en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 25, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

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

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

c) la naturaleza de los datos personales, en concreto si se tratan categorías especiales de datos personales, de conformidad con el artículo 10, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 11;

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

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

Artículo 7

Condiciones para el consentimiento

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

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

3. El interesado tendrá derecho a revocar su consentimiento en cualquier momento. La revocación del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su revocación. Antes de prestar su consentimiento, el interesado será informado de ello. Será tan fácil revocar el consentimiento como prestarlo.

4. Al evaluar si el consentimiento se ha prestado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, el cumplimiento de un contrato, incluida la prestación de un servicio, se supedita a consentir el tratamiento de datos personales que son innecesarios para el cumplimiento de dicho contrato.

Artículo 8

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

1. Cuando se aplique el artículo 5, apartado 1, letra d), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 13 años. Si el niño es menor de 13 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo prestó o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se prestó o autorizó.

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

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

Artículo 9

Transmisiones de datos personales a destinatarios establecidos en la Unión distintos de las instituciones y organismos de la Unión

1. Sin perjuicio de lo dispuesto en los artículos 4 a 6 y 10, los datos personales solo se transmitirán a destinatarios establecidos en la Unión distintos de las instituciones y organismos de la Unión, cuando:

a) el destinatario demuestre que los datos son necesarios para el cumplimiento de una función de interés público o en el ejercicio de las potestades públicas conferidas al destinatario, o

b) el destinatario demuestre que es necesario que le transmitan los datos para una finalidad específica de interés público y el responsable del tratamiento, si existe alguna razón para suponer que se podrían perjudicar los intereses legítimos del interesado, demuestre que es proporcionado transmitir los datos personales para dicha finalidad específica, una vez sopesados, de modo verificable, los diversos intereses concurrentes.

2. Cuando la transmisión según el presente artículo se produzca por iniciativa del responsable del tratamiento, este deberá demostrar que la transmisión de datos personales es necesaria y proporcionada respecto de los fines de la transmisión, mediante la aplicación de los criterios establecidos en el apartado 1, letras a) o b).

3. Las instituciones y organismos de la Unión conciliarán el derecho a la protección de los datos personales con el derecho de acceso a los documentos, de conformidad con el Derecho de la Unión.

Artículo 10

Tratamiento de categorías especiales de datos personales

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

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

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

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice una normativa de la Unión que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado,

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

d) el tratamiento lo lleva a cabo, en el ejercicio de sus actividades legítimas y con las garantías apropiadas, un organismo sin ánimo de lucro que constituya una entidad integrada en una institución u organismo de la Unión y cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a sus miembros, a antiguos miembros del organismo o a personas que mantengan contactos regulares con este en relación con sus fines y siempre que los datos no se comuniquen fuera del organismo sin el consentimiento de los interesados;

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

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando el Tribunal de Justicia actúe en ejercicio de su función judicial,

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

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

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

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos sobre la base de una normativa de la Unión que debe ser proporcionada respecto del objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

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

Artículo 11

Tratamiento de datos personales relativos a condenas e infracciones penales

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas basadas en el artículo 5, apartado 1, solo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice una normativa de la Unión que establezca garantías adecuadas para los derechos y libertades de los interesados.

Artículo 12

Tratamiento que no requiere identificación

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

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 17 a 22, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

Artículo 13

Garantías aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

CAPÍTULO III

DERECHOS DEL INTERESADO

SECCIÓN 1

transparencia y modalidades

Artículo 14

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

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 15 y 16, así como cualquier comunicación con arreglo a los artículos 17 a 24 y 35 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 17 a 24. En los casos a que se refiere el artículo 12, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 17 a 24, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado, sin dilaciones indebidas y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud, información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 17 a 24. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no atiende a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes a partir de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante el Supervisor Europeo de Protección de Datos y de interponer un recurso judicial.

5. La información facilitada en virtud de los artículos 15 y 16 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 17 a 24 y 35 serán proporcionadas gratuitamente. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 12, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que efectúa la solicitud a que se refieren los artículos 17 a 23, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que debe facilitarse a los interesados en virtud de los artículos 15 y 16 podrá transmitirse en combinación con iconos normalizados, para proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. Si la Comisión adopta actos delegados en virtud del artículo 12, apartado 8, del Reglamento (UE) 2016/679 por los que se especifique la información que se ha de presentar a través de los iconos y los procedimientos para proporcionar iconos normalizados, las instituciones y organismos de la Unión facilitarán, en su caso, la información en virtud de los artículos 15 y 16 del presente Reglamento junto con dichos iconos normalizados.

SECCIÓN 2

información y acceso a los datos personales

Artículo 15

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

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

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

b) los datos de contacto del delegado de protección de datos;

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

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

e) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en el artículo 48, referencia a las garantías adecuadas o idóneas y a los medios para obtener una copia de estas o al lugar en el que estén disponibles.

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

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

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

c) cuando el tratamiento esté basado en el artículo 5, apartado 1, letra d), o el artículo 10, apartado 2, letra a), la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su revocación;

d) el derecho a presentar una reclamación ante el Supervisor Europeo de Protección de Datos;

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

f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 24, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

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

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

Artículo 16

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

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

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

b) los datos de contacto del delegado de protección de datos;

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

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

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

f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en el artículo 48, referencia a las garantías adecuadas o idóneas y a los medios para obtener una copia de ellas o al lugar en el que estén disponibles.

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

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

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

c) cuando el tratamiento esté basado en el artículo 5, apartado 1, letra d), o el artículo 10, apartado 2, letra a), la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su revocación;

d) el derecho a presentar una reclamación ante el Supervisor Europeo de Protección de Datos;

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

f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 24, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

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

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

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

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

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

5. Los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento;

c) la obtención o la comunicación esté expresamente establecida por una normativa de la Unión que establezca medidas adecuadas para proteger los intereses legítimos del interesado; o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de un deber de secreto profesional regulado por el Derecho de la Unión, incluida una obligación legal de secreto.

6. En los casos mencionados en el apartado 5, letra b), el responsable del tratamiento adoptará medidas adecuadas para proteger los derechos, las libertades y los intereses legítimos del interesado, también haciendo pública la información.

Artículo 17

Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

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

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros países u organizaciones internacionales;

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

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

f) el derecho a presentar una reclamación ante el Supervisor Europeo de Protección de Datos;

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

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 24, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 48 relativas a la transferencia.

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

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

SECCIÓN 3

rectificación y supresión

Artículo 18

Derecho de rectificación

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

Artículo 19

Derecho de supresión («derecho al olvido»)

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

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

b) el interesado revoque el consentimiento en que se basa el tratamiento de conformidad con el artículo 5, apartado 1, letra d), o el artículo 10, apartado 2, letra a), y este no tenga ninguna otra base jurídica;

c) el interesado se oponga al tratamiento con arreglo al artículo 23, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento;

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

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

3. Los apartados 1 y 2 no serán aplicables el tratamiento sea necesario:

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

b) para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento, o para el cumplimiento de una función realizada en interés público o en el ejercicio de potestades públicas conferidas al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 10, apartado 2, letras h) e i), y apartado 3;

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

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

Artículo 20

Derecho a la limitación del tratamiento

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

a) el interesado impugne la exactitud de los datos personales, en un plazo que permita al responsable verificar que son exactos y que están completos;

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

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

d) el interesado se haya opuesto al tratamiento en virtud del artículo 23, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

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

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

4. En los ficheros automatizados, la limitación del tratamiento deberá realizarse, en principio, por medios técnicos. El hecho de que los datos personales están limitados se indicará en el sistema de tal modo que quede claro que no se pueden utilizar.

Artículo 21

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

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 18, al artículo 19, apartado 1, y al artículo 20 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si el interesado así lo solicita.

Artículo 22

Derecho a la portabilidad de los datos

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

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 5, apartado 1, letra d), o el artículo 10, apartado 2, letra a), o en un contrato con arreglo al artículo 5, apartado 1, letra c); y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, o a responsables del tratamiento distintos de las instituciones y organismos de la Unión, cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 19. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de potestades públicas conferidas al responsable del tratamiento.

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

SECCIÓN 4

derecho de oposición y decisiones individuales automatizadas

Artículo 23

Derecho de oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 5, apartado 1, letra a), incluida la elaboración de perfiles sobre la base de dicha disposición. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

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

3. Sin perjuicio de lo dispuesto en los artículos 36 y 37, en el contexto de la utilización de servicios de la sociedad de la información, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

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

Artículo 24

Decisiones individuales automatizadas, incluida la elaboración de perfiles

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

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

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

b) está autorizada por una normativa de la Unión que establezca asimismo medidas adecuadas para salvaguardar los derechos y las libertades y los intereses legítimos del interesado; o

c) se basa en el consentimiento expreso del interesado.

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

4. Las decisiones a que se refiere el apartado 2 del presente artículo no se basarán en las categorías especiales de datos personales mencionadas en el artículo 10, apartado 1, salvo que se aplique el artículo 10, apartado 2, letras a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

SECCIÓN 5

limitaciones

Artículo 25

Limitaciones

1. Los actos jurídicos adoptados con arreglo a los Tratados o, en cuestiones relacionadas con el funcionamiento de las instituciones y organismos de la Unión, las normas internas establecidas por estos últimos podrán limitar la aplicación de los artículos 14 a 22, 35 y 36, y también del artículo 4 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones que disponen los artículos 14 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad nacional, el orden público o la defensa de los Estados miembros;

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

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

d) la seguridad interna de las instituciones y organismos de la Unión, incluida la de sus redes de comunicación electrónica;

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

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

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

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

i) la ejecución de demandas civiles.

2. En particular, cualquier acto jurídico o norma interna indicados en el apartado 1 contendrá, en su caso, disposiciones específicas relativas a:

a) las finalidades del tratamiento o de las categorías de tratamiento;

b) las categorías de datos personales;

c) el alcance de las limitaciones establecidas;

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

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

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

g) los riesgos para los derechos y las libertades de los interesados.

3. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos, el Derecho de la Unión, que puede incluir normas internas adoptadas por las instituciones y organismos de la Unión en cuestiones relacionadas con su funcionamiento, podrá establecer excepciones a los derechos reconocidos en los artículos 17, 18, 20 y 23, sujetas a las condiciones y garantías indicadas en el artículo 13, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines específicos, y que esas excepciones sean necesarias para alcanzar esos fines.

4. Cuando se traten datos personales con fines de archivo en interés público, el Derecho de la Unión, que puede incluir normas internas adoptadas por las instituciones y organismos de la Unión en cuestiones relacionadas con su funcionamiento, podrá establecer excepciones a los derechos reconocidos en los artículos 17, 18, 20, 21, 22 y 23, sujetas a las condiciones y garantías indicadas en el artículo 13, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines específicos, y que esas excepciones sean necesarias para alcanzar esos fines.

5. Las normas internas mencionadas en los apartados 1, 3 y 4 serán actos de aplicación general claros y precisos, destinados a producir efectos jurídicos respecto de los interesados, adoptados al nivel de gestión más elevado de las instituciones y organismos de la Unión y deben ser objeto de su publicación en el *Diario Oficial de la Unión Europea*.

6. En caso de que se imponga una limitación en virtud del apartado 1, se informará al interesado, de conformidad con el Derecho de la Unión, de las razones principales que justifican la limitación, así como de su derecho a presentar una reclamación ante el Supervisor Europeo de Protección de Datos.

7. En caso de que se invoque una limitación aplicada en virtud del apartado 1 para denegar al interesado el acceso a los datos, el Supervisor Europeo de Protección de Datos, durante la investigación de la reclamación, solo le comunicará si los datos se trataron correctamente y, de no ser así, si se han efectuado las correcciones necesarias.

8. Podrá aplazarse, omitirse o denegarse la comunicación de la información a la que se refieren los apartados 6 y 7 del presente artículo y el artículo 45, apartado 2, si dicha comunicación dejase sin efecto la limitación impuesta sobre la base del apartado 1 del presente artículo.

CAPÍTULO IV

RESPONSABLE DEL TRATAMIENTO Y ENCARGADO DEL TRATAMIENTO

SECCIÓN 1

obligaciones generales

Artículo 26

Responsabilidad del responsable del tratamiento

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

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

3. Podrá utilizarse la adhesión a mecanismos de certificación aprobados como menciona el artículo 42 del Reglamento (UE) 2016/679 como elemento para acreditar el cumplimiento de las obligaciones que incumben al responsable del tratamiento.

Artículo 27

Protección de datos desde el diseño y por defecto

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

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

3. Podrá utilizarse un mecanismo de certificación aprobado como menciona el artículo 42 del Reglamento (UE) 2016/679 como elemento para acreditar el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Artículo 28

Corresponsables del tratamiento

1. Cuando dos o más responsables del tratamiento o uno o más responsables junto con otro u otros responsables del tratamiento distintos de las instituciones y organismos de la Unión, determinen conjuntamente los objetivos y medios del tratamiento, serán considerados corresponsables del tratamiento. Los corresponsables del tratamiento determinarán de modo transparente sus responsabilidades respectivas en el cumplimiento de sus obligaciones en materia de protección de datos, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de facilitar la información a que se refieren los artículos 15 y 16, mediante un acuerdo entre ellos, salvo que, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que les sea aplicable. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo mencionado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas que los corresponsables del tratamiento tengan respecto de los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

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

Artículo 29

Encargado del tratamiento

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

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

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

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

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

c) tome todas las medidas necesarias de conformidad con el artículo 33;

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

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

f) ayude al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 33 a 41, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

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

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

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

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

5. Cuando el encargado del tratamiento no sea una institución u organismo de la Unión, su adhesión a un código de conducta aprobado a que se refiere el artículo 40, apartado 5, del Reglamento (UE) 2016/679 o a un mecanismo de certificación aprobado a que se refiere el artículo 42 de dicho Reglamento podrá utilizarse como elemento para demostrar la existencia de garantías suficientes como disponen los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable del tratamiento y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al encargado que no sea una institución u organismo de la Unión de conformidad con el artículo 42 del Reglamento (UE) 2016/679.

7. La Comisión podrá fijar cláusulas contractuales tipo para las cuestiones a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 96, apartado 2.

8. El Supervisor Europeo de Protección de Datos podrá adoptar cláusulas contractuales tipo para las cuestiones a que se refieren los apartados 3 y 4.

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

10. Sin perjuicio de lo dispuesto en los artículos 65 y 66, si un encargado del tratamiento infringe el presente Reglamento por determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 30

Tratamiento bajo la autoridad del responsable del tratamiento o del encargado del tratamiento

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

Artículo 31

Registro de las actividades de tratamiento

1. Cada responsable llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

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

b) los fines del tratamiento;

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

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

e) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y la documentación de garantías adecuadas;

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

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 33.

2. Cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados del tratamiento y de cada responsable del tratamiento en cuyo nombre actúe el encargado, y del delegado de protección de datos;

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

c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y la documentación de garantías adecuadas;

d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 33.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, valiendo también el formato electrónico.

4. Las instituciones y organismos de la Unión pondrán el registro a disposición del Supervisor Europeo de Protección de Datos cuando este lo solicite.

5. Salvo que no sea adecuado habida cuenta del tamaño de la institución u organismo de la Unión, las instituciones y organismos de la Unión mantendrán sus registros de actividades de tratamiento en un registro central. Harán que el registro sea de acceso público.

Artículo 32

Cooperación con el Supervisor Europeo de Protección de Datos

Las instituciones y organismos de la Unión cooperarán con el Supervisor Europeo de Protección de Datos en el desempeño de sus funciones cuando este lo solicite.

SECCIÓN 2

seguridad de los datos personales

Artículo 33

Seguridad del tratamiento

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

a) la seudonimización y el cifrado de datos personales;

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

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

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

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

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

4. Podrá utilizarse la adhesión a un mecanismo de certificación aprobado como menciona el artículo 42 del Reglamento (UE) 2016/679 como elemento para acreditar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo.

Artículo 34

Notificación de una violación de la seguridad de los datos personales al Supervisor Europeo de Protección de Datos

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará al Supervisor Europeo de Protección de Datos sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación al Supervisor Europeo de Protección de Datos no tiene lugar 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 mencionada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, incluidos, 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;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

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

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

5. El responsable del tratamiento informará al delegado de protección de datos acerca de la violación de la seguridad de los datos.

6. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá al Supervisor Europeo de Protección de Datos verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 35

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

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

2. La comunicación al interesado a que se refiere el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 34, apartado 3, letras b), c) y d).

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

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

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

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

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

SECCIÓN 3

confidencialidad de las comunicaciones electrónicas

Artículo 36

Confidencialidad de las comunicaciones electrónicas

Las instituciones y organismos de la Unión garantizarán la confidencialidad de las comunicaciones electrónicas, en particular protegiendo sus redes de comunicación electrónica.

Artículo 37

Protección de la información transmitida a los equipos terminales de los usuarios, almacenada en dichos equipos, relativa a ellos, tratada por ellos y recopilada de ellos

Respecto de los usuarios que accedan a los sitios web de acceso público y aplicaciones para móviles de las instituciones y organismos de la Unión, estas instituciones y organismos protegerán la información transmitida a los equipos terminales de dichos usuarios, la información almacenada en esos equipos, relacionada con ellos, tratada por ellos y recogida de ellos, de conformidad con el artículo 5, apartado 3, de la Directiva 2002/58/CE.

Artículo 38

Guías de usuarios

1. Los datos personales contenidos en las guías de usuarios y el acceso a dichas guías quedarán limitados a lo necesario para los fines específicos de la guía.

2. Las instituciones y organismos de la Unión adoptarán las medidas necesarias para evitar que los datos personales contenidos en estas guías, independientemente de si resultan accesibles al público o no, sean utilizados para fines de venta directa.

SECCIÓN 4

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

Artículo 39

Evaluación de impacto relativa a la protección de datos

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

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

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

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

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 10 o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 11; o

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

4. El Supervisor Europeo de Protección de Datos establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1.

5. El Supervisor Europeo de Protección de Datos podrá asimismo establecer y publicar una lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5 del presente artículo, el Supervisor Europeo de Protección de Datos solicitará que el Comité Europeo de Protección de Datos establecido por el artículo 68 del Reglamento (UE) 2016/679 examine dichas listas de conformidad con el artículo 70, apartado 1, letra e), de dicho Reglamento cuando se refieran a las operaciones de tratamiento por parte de un responsable del tratamiento que actúe conjuntamente con uno o más responsables del tratamiento distintos de las instituciones y organismos de la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento;

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

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

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

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 del Reglamento (UE) 2016/679 por los encargados correspondientes que no sean instituciones u organismos de la Unión se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 5, apartado 1, letras a) o b), tenga su base jurídica en un acto jurídico adoptado sobre la base de los Tratados, que regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y cuando ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general anterior a la adopción de dicho acto jurídico, los apartados 1 a 6 del presente artículo no serán de aplicación salvo que se establezca de otro modo en dicho acto jurídico.

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

Artículo 40

Consulta previa

1. El responsable consultará al Supervisor Europeo de Protección de Datos antes de proceder al tratamiento si una evaluación de impacto relativa a la protección de datos en virtud del artículo 39 muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables teniendo en cuenta la tecnología disponible y los costes de aplicación. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos acerca de la necesidad de una consulta previa.

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

3. Cuando consulte al Supervisor Europeo de Protección de Datos con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento;

b) los fines y medios del tratamiento previsto;

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

d) los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 39; y

f) cualquier otra información que solicite el Supervisor Europeo de Protección de Datos.

4. La Comisión podrá determinar, mediante un acto de ejecución, una lista de los casos en los que los responsables del tratamiento consultarán al Supervisor Europeo de Protección de Datos y recabarán su autorización previa en relación con el tratamiento de datos personales por un responsable en el ejercicio de una función realizada en interés público, en particular el tratamiento de dichos datos en relación con la protección social y la salud pública.

SECCIÓN 5

información y consulta legislativa

Artículo 41

Información y consulta

1. Las instituciones y organismos de la Unión informarán al Supervisor Europeo de Protección de Datos cuando elaboren medidas administrativas y normas internas relacionadas con el tratamiento de datos personales por parte de una institución u organismo de la Unión, ya sea aisladamente o junto con otros.

2. Las instituciones y organismos de la Unión consultarán al Supervisor Europeo de Protección de Datos cuando elaboren las normas internas a que se refiere el artículo 25.

Artículo 42

Consulta legislativa

1. Tras la adopción de propuestas de actos legislativos, de recomendaciones o de propuestas al Consejo en virtud del artículo 218 del TFUE, o cuando prepare actos delegados o actos de ejecución, la Comisión consultará al Supervisor Europeo de Protección de Datos cuando tengan repercusiones sobre la protección de los derechos y libertades de las personas en relación con el tratamiento de datos personales.

2. Cuando uno de los actos mencionados en el apartado 1 sea de especial importancia para la protección de los derechos y libertades de las personas en relación con el tratamiento de datos personales, la Comisión podrá consultar al Comité Europeo de Protección de Datos. En estos casos, el Supervisor Europeo de Protección de Datos y el Comité Europeo de Protección de Datos coordinarán su trabajo a fin de emitir un dictamen conjunto.

3. El asesoramiento mencionado en los apartados 1 y 2 será facilitado por escrito en un plazo de hasta ocho semanas desde la solicitud de la consulta mencionada en los apartados 1 y 2. En casos urgentes, o cuando se considere conveniente, la Comisión podrá acortar este plazo.

4. El presente artículo no será aplicable cuando la Comisión, de conformidad con el Reglamento (UE) 2016/679, deba consultar al Comité Europeo de Protección de Datos.

SECCIÓN 6

delegado de protección de datos

Artículo 43

Designación del delegado de protección de datos

1. Cada institución u organismo de la Unión designará un delegado de protección de datos.

2. Las instituciones y organismos de la Unión pueden designar a un único delegado de protección de datos para varias de ellas, teniendo en cuenta su estructura organizativa y tamaño.

3. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 45.

4. El delegado de protección de datos formará parte de la plantilla de la institución u organismo de la Unión. Teniendo en cuenta su tamaño y si no se ejerce la facultad que dispone el apartado 2, las instituciones y organismos de la Unión podrán designar un delegado de protección de datos que desempeñe sus funciones en el marco de un contrato de servicios.

5. Las instituciones y organismos de la Unión publicarán los datos de contacto del delegado de protección de datos y los comunicarán al Supervisor Europeo de Protección de Datos.

Artículo 44

Posición del delegado de protección de datos

1. Las instituciones y organismos de la Unión garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. Las instituciones y organismos de la Unión respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 45, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

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

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

5. El delegado de protección de datos y su personal estarán obligados a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión.

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

7. El delegado de protección de datos podrá ser consultado por el responsable del tratamiento y el encargado del tratamiento, por el comité de personal afectado y por cualquier persona, sobre cualquier cuestión que se refiera a la interpretación o aplicación del presente Reglamento, sin necesidad de seguir los conductos oficiales. Nadie deberá sufrir perjuicio alguno por informar al delegado competente de protección de datos de que se ha cometido una infracción de lo dispuesto en el presente Reglamento.

8. El delegado de protección de datos será designado por un mandato de entre tres y cinco años y este podrá ser renovado. En caso de que deje de cumplir las condiciones requeridas para el ejercicio de sus funciones, el delegado de protección de datos podrá ser destituido de su cargo por la institución u organismo de la Unión que le haya designado solo previo consentimiento del Supervisor Europeo de Protección de Datos.

9. Tras haber designado al delegado de protección de datos, la institución u organismo de la Unión que le haya designado comunicará su nombre al Supervisor Europeo de Protección de Datos.

Artículo 45

Funciones del delegado de protección de datos

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

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

b) garantizar de forma independiente la aplicación interna del presente Reglamento y supervisar el cumplimiento del presente Reglamento, de otras normas aplicables de la Unión que contengan disposiciones de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) velar por que los interesados sean informados de sus derechos y obligaciones con arreglo al presente Reglamento;

d) ofrecer el asesoramiento que se le solicite acerca de la necesidad de notificar o comunicar una violación de la seguridad de los datos personales con arreglo a los artículos 34 y 35;

e) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 39 y consultar al Supervisor Europeo de Protección de Datos en caso de duda sobre la necesidad de una evaluación de impacto relativa a la protección de datos;

f) ofrecer el asesoramiento que se le solicite acerca de la necesidad de una consulta previa del Supervisor Europeo de Protección de Datos de conformidad con el artículo 40; consultar a este en caso de duda sobre la necesidad de una consulta previa;

g) responder a las solicitudes del Supervisor Europeo de Protección de Datos; en el marco de sus competencias, cooperar y consultar con el Supervisor Europeo de Protección de Datos a petición de este o por iniciativa propia;

h) velar por que las operaciones de tratamiento no tengan efectos adversos sobre los derechos y las libertades de los interesados.

2. El delegado de protección de datos podrá formular recomendaciones al responsable del tratamiento y al encargado del tratamiento, para la mejora práctica de la protección de datos y aconsejarles sobre cuestiones relativas a la puesta en práctica de las disposiciones sobre protección de datos. Por otra parte, por iniciativa propia o a petición del responsable o del encargado del tratamiento, del comité de personal afectado o de cualquier persona física, podrá investigar las cuestiones y los incidentes directamente relacionados con sus funciones que lleguen a su conocimiento e informar de ello a la persona que solicitó la investigación o al responsable o al encargado del tratamiento.

3. Cada institución u organismo de la Unión adoptará normas complementarias respecto al delegado de protección de datos. Las normas de aplicación se referirán en especial a las tareas, funciones y competencias del delegado de protección de datos.

CAPÍTULO V

TRANSFERENCIAS DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

Artículo 46

Principio general de las transferencias

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

Artículo 47

Transferencias basadas en una decisión de adecuación

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido, en virtud del artículo 45, apartado 3, del Reglamento (UE) 2016/679, o del artículo 36, apartado 3, de la Directiva (UE) 2016/680, 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 y cuando los datos se transfieran exclusivamente para permitir el ejercicio de funciones que sean competencia del responsable del tratamiento.

2. Las instituciones y organismos de la Unión informarán a la Comisión y al Supervisor Europeo de Protección de Datos de los casos en los que consideren que un tercer país, territorio o uno o varios sectores específicos de un tercer país, o una organización internacional de que se trate no garantizan un nivel de protección adecuado de acuerdo con el apartado 1.

3. Las instituciones y organismos de la Unión tomarán las medidas necesarias para cumplir las decisiones adoptadas por la Comisión cuando esta determine, en aplicación del artículo 45, apartados 3 o 5, del Reglamento (UE) 2016/679 o del artículo 36, apartados 3 o 5, de la Directiva (UE) 2016/680, que un tercer país, territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan o ya no garantizan un nivel de protección adecuado.

Artículo 48

Transferencias mediante garantías adecuadas

1. A falta de una decisión con arreglo al artículo 45, apartado 3, del Reglamento (UE) 2016/679, o al artículo 36, apartado 3, de la Directiva (UE) 2016/680, el responsable del tratamiento o el encargado del tratamiento solo podrá transferir datos personales a un tercer país o a una organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa del Supervisor Europeo de Protección de Datos, por los medios siguientes:

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

b) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 96, apartado 2;

c) cláusulas tipo de protección de datos adoptadas por el Supervisor Europeo de Protección de Datos y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 96, apartado 2;

d) cuando el encargado del tratamiento no sea una institución u organismo de la Unión, normas corporativas vinculantes, códigos de conducta o mecanismos de certificación con arreglo al artículo 46, apartado 2, letras b), e) y f), del Reglamento (UE) 2016/679.

3. Siempre que exista autorización del Supervisor Europeo de Protección de Datos, las garantías adecuadas referidas en el apartado 1 también podrán ser aportadas, en particular, mediante:

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

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

4. Las autorizaciones concedidas por el Supervisor Europeo de Protección de Datos de conformidad con el artículo 9, apartado 7, del Reglamento (CE) n.º 45/2001 seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por este.

5. Las instituciones y organismos de la Unión informarán al Supervisor Europeo de Protección de Datos de las categorías de casos en que el presente artículo haya sido aplicado.

Artículo 49

Transferencias o comunicaciones no autorizadas por el Derecho de la Unión

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

Artículo 50

Excepciones para situaciones específicas

1. A falta de una decisión de adecuación de conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679, o el artículo 36, apartado 3, de la Directiva (UE) 2016/680, o de garantías adecuadas de conformidad con el artículo 48 del presente Reglamento, solo podrá realizarse una transferencia o una serie de transferencias de datos personales a un tercer país o una organización internacional si se cumple alguna de las condiciones siguientes:

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

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

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

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

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

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

g) la transferencia se realice desde un registro que, con arreglo al Derecho de la Unión, tenga por objeto proporcionar información al público y que esté disponible para consulta del público en general o de cualquier persona que pueda demostrar un interés legítimo, pero solo en la medida en que en ese caso particular se cumplan las condiciones que establece el Derecho de la Unión para la consulta.

2. Las letras a), b) y c) del apartado 1 no serán aplicables a las actividades llevadas a cabo por las instituciones y organismos de la Unión en el ejercicio de sus potestades públicas.

3. El interés público indicado en el apartado 1, letra d), será reconocido por el Derecho de la Unión.

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

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

6. Las instituciones y organismos de la Unión informarán al Supervisor Europeo de Protección de Datos de las categorías de casos en que el presente artículo haya sido aplicado.

Artículo 51

Cooperación internacional en el ámbito de la protección de datos personales

En relación con los terceros países y las organizaciones internacionales, el Supervisor Europeo de Protección de Datos, en cooperación con la Comisión y el Comité Europeo de Protección de Datos, tomará medidas apropiadas para:

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

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

c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

CAPÍTULO VI

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Artículo 52

Supervisor Europeo de Protección de Datos

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

2. Por lo que respecta al tratamiento de los datos personales, el Supervisor Europeo de Protección de Datos velará por que los derechos y libertades fundamentales de las personas físicas, en particular el derecho de las mismas a la protección de datos, sean respetados por las instituciones y organismos de la Unión.

3. El Supervisor Europeo de Protección de Datos garantizará y supervisará la aplicación de las disposiciones del presente Reglamento y de cualquier otro acto de la Unión relacionado con la protección de los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento de datos personales por parte de una institución u organismo de la Unión, y asesorará a las instituciones y organismos de la Unión, así como a los interesados, en todas las cuestiones relacionadas con el tratamiento de datos personales. Con este fin, el Supervisor Europeo de Protección de Datos ejercerá las funciones establecidas en el artículo 57 y las competencias que le confiere el artículo 58.

4. El Reglamento (CE) n.º 1049/2001 se aplicará a los documentos que estén en poder del Supervisor Europeo de Protección de Datos. El Supervisor Europeo de Protección de Datos adoptará las normas de aplicación del Reglamento (CE) n.º 1049/2001 con respecto a dichos documentos.

Artículo 53

Nombramiento del Supervisor Europeo de Protección de Datos

1. El Parlamento Europeo y el Consejo nombrarán de común acuerdo al Supervisor Europeo de Protección de Datos por un mandato de cinco años, sobre la base de una lista elaborada por la Comisión como resultado de una convocatoria pública de candidaturas. La convocatoria de candidaturas permitirá a las partes interesadas de toda la Unión presentar sus candidaturas. La lista de candidatos será pública y constará como mínimo de tres candidatos. Sobre la base de la lista elaborada por la Comisión, la comisión competente del Parlamento Europeo podrá decidir la celebración de una audiencia con objeto de definir una preferencia.

2. La lista de candidatos a que se refiere el apartado 1 estará compuesta por personas cuya independencia esté fuera de toda duda y que posean un conocimiento especializado en protección de datos, así como de la experiencia y competencia necesarias para el cumplimiento de las funciones de Supervisor Europeo de Protección de Datos.

3. El mandato del Supervisor Europeo de Protección de Datos será renovable una sola vez.

4. El mandato del Supervisor Europeo de Protección de Datos llegará a su fin en las siguientes circunstancias:

a) si el Supervisor Europeo de Protección de Datos es sustituido;

b) si el Supervisor Europeo de Protección de Datos dimite;

c) si el Supervisor Europeo de Protección de Datos es despedido u obligado a jubilarse.

5. El Supervisor Europeo de Protección de Datos podrá ser destituido o desposeído de su derecho de pensión u otros privilegios equivalentes por el Tribunal de Justicia a petición del Parlamento Europeo, el Consejo o la Comisión si dejare de cumplir las condiciones necesarias para el ejercicio de sus funciones o hubiere cometido una falta grave.

6. En los casos de renovación periódica y dimisión voluntaria, el Supervisor Europeo de Protección de Datos permanecerá en funciones hasta su sustitución.

7. Los artículos 11 a 14 y 17 del Protocolo sobre los privilegios y las inmunidades de la Unión Europea serán aplicables al Supervisor Europeo de Protección de Datos.

Artículo 54

Estatuto y condiciones generales de ejercicio de las funciones de Supervisor Europeo de Protección de Datos, personal y recursos financieros

1. El Supervisor Europeo de Protección de Datos recibirá la misma consideración que un juez del Tribunal de Justicia en cuanto a la determinación de su salario, asignaciones, pensión de jubilación y demás ventajas de carácter retributivo.

2. La autoridad presupuestaria garantizará que el Supervisor Europeo de Protección de Datos disponga de los recursos humanos y financieros necesarios para el ejercicio de sus funciones.

3. El presupuesto del Supervisor Europeo de Protección de Datos figurará en una línea propia de la sección del presupuesto general de la Unión dedicada a los gastos administrativos.

4. El Supervisor Europeo de Protección de Datos estará asistido por una secretaría. Los funcionarios y otros miembros del personal de la secretaría serán nombrados por el Supervisor Europeo de Protección de Datos, que será su superior jerárquico. Estarán sometidos exclusivamente a su dirección. El número de puestos se decidirá anualmente en el marco del procedimiento presupuestario. Al personal del Supervisor Europeo de Protección de Datos que participe en la realización de las funciones atribuidas al Comité Europeo de Protección de Datos por el Derecho de la Unión se le aplicará el artículo 75, apartado 2, del Reglamento (UE) 2016/679.

5. Los funcionarios y otros miembros del personal de la secretaría del Supervisor Europeo de Protección de Datos estarán sujetos a los reglamentos y normas aplicables a los funcionarios y otros agentes de la Unión.

6. El Supervisor Europeo de Protección de Datos tendrá su sede en Bruselas.

Artículo 55

Independencia

1. El Supervisor Europeo de Protección de Datos actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus competencias de conformidad con el presente Reglamento.

2. El Supervisor Europeo de Protección de Datos será ajeno, en el desempeño de sus funciones y en el ejercicio de sus potestades de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitará ni admitirá ninguna instrucción.

3. El Supervisor Europeo de Protección de Datos se abstendrá de cualquier acción incompatible con sus funciones y de desempeñar, durante su mandato, ninguna otra actividad profesional, sea o no retribuida.

4. Tras la finalización de su mandato, el Supervisor Europeo de Protección de Datos actuará con integridad y discreción en lo que respecta a la aceptación de nombramientos y privilegios.

Artículo 56

Secreto profesional

El Supervisor Europeo de Protección de Datos y su personal estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre las informaciones confidenciales a las que hayan tenido acceso durante el ejercicio de sus funciones.

Artículo 57

Funciones

1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá al Supervisor Europeo de Protección de Datos:

a) supervisar y garantizar la aplicación del presente Reglamento por parte de las instituciones y organismos de la Unión, con excepción del tratamiento de datos personales por el Tribunal de Justicia cuando actúe en el ejercicio de sus funciones jurisdiccionales;

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

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

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

e) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 67, 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;

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

g) asesorar, por iniciativa propia o previa solicitud, a todas las instituciones y organismos de la Unión sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales;

h) hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación;

i) adoptar las cláusulas contractuales tipo a que se refieren el artículo 29, apartado 8, y el artículo 48, apartado 2, letra c);

j) elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 39, apartado 4;

k) participar en las actividades del Comité Europeo de Protección de Datos;

l) facilitar una secretaría al Comité Europeo de Protección de Datos, de conformidad con el artículo 75 del Reglamento (UE) 2016/679;

m) ofrecer asesoramiento sobre el tratamiento contemplado en el artículo 40, apartado 2;

n) autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 48, apartado 3;

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

p) desempeñar cualquier otra función relacionada con la protección de los datos personales; y

q) adoptar su reglamento interno.

2. El Supervisor Europeo de Protección de Datos facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra e), mediante un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

3. El desempeño de las funciones del Supervisor Europeo de Protección de Datos será gratuito para el interesado.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el Supervisor Europeo de Protección de Datos podrá negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en el Supervisor Europeo de Protección de Datos.

Artículo 58

Potestades

1. El Supervisor Europeo de Protección de Datos dispondrá de las potestades de investigación indicados a continuación:

a) ordenar al responsable y al encargado del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones;

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

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

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

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

2. El Supervisor Europeo de Protección de Datos dispondrá de las potestades correctivas indicadas a continuación:

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

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

c) someter asuntos al responsable o encargado del tratamiento de que se trate y, en su caso, al Parlamento Europeo, al Consejo y a la Comisión;

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

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

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

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

h) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 18, 19 y 20 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo al artículo 19, apartado 2, y al artículo 21;

i) imponer una multa administrativa con arreglo al artículo 66, en caso de incumplimiento por parte de una institución u organismo de la Unión de alguna de las medidas mencionadas en las letras (d) a (h) y (j) del presente apartado, en función de las circunstancias de cada caso particular;

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

3. El Supervisor Europeo de Protección de Datos dispondrá de las potestades de autorización y consultivos indicados a continuación:

a) asesorar a los interesados en el ejercicio de sus derechos;

b) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa que menciona el artículo 40, y de acuerdo con el artículo 41, apartado 2;

c) emitir, por iniciativa propia o previa solicitud, dictámenes destinados a las instituciones y organismos de la Unión y al público, sobre cualquier asunto relacionado con la protección de los datos personales;

d) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 29, apartado 8, y el artículo 48, apartado 2, letra c);

e) autorizar las cláusulas contractuales indicadas en el artículo 48, apartado 3, letra a);

f) autorizar los acuerdos administrativos contemplados en el artículo 48, apartado 3, letra b);

g) autorizar las operaciones de tratamiento con arreglo a actos de ejecución adoptados de conformidad con el artículo 40, apartado 4.

4. El Supervisor Europeo de Protección de Datos estará facultado para someter un asunto al Tribunal de Justicia en las condiciones previstas en los Tratados e intervenir en los asuntos presentados ante dicho Tribunal.

5. El ejercicio de las potestades conferidas al Supervisor Europeo de Protección de Datos en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y el respeto de las garantías procesales, establecidas en el Derecho de la Unión.

Artículo 59

Obligación de los responsables y encargados del tratamiento de responder a las alegaciones

Cuando el Supervisor Europeo de Protección de Datos ejerza las facultades establecidas en el artículo 58, apartado 2, letras a), b) y c), el responsable del tratamiento o encargado del tratamiento en cuestión le comunicará su opinión en un plazo razonable fijado por el Supervisor Europeo de Protección de Datos, teniendo en cuenta las circunstancias de cada caso. La respuesta comprenderá asimismo una descripción de las medidas adoptadas, en su caso, a raíz de las observaciones del Supervisor Europeo de Protección de Datos.

Artículo 60

Informe de actividad

1. El Supervisor Europeo de Protección de Datos presentará anualmente al Parlamento Europeo, al Consejo y a la Comisión un informe sobre sus actividades, que paralelamente hará público.

2. El Supervisor Europeo de Protección de Datos transmitirá el informe al que se refiere el apartado 1 a las demás instituciones y organismos de la Unión, los cuales podrán presentar comentarios con vistas a un posible examen del informe por parte del Parlamento Europeo.

CAPÍTULO VII

COOPERACIÓN Y COHERENCIA

Artículo 61

Cooperación entre el Supervisor Europeo de Protección de Datos y las autoridades de control nacionales

El Supervisor Europeo de Protección de Datos cooperará con las autoridades de control nacionales y con la Autoridad de Supervisión Común creada por el artículo 25 de la Decisión 2009/917/JAI del Consejo ([1]) en la medida necesaria para el ejercicio de sus respectivas funciones, en particular intercambiando entre sí información pertinente, se instarán mutuamente a ejercer sus potestades y responderán a las solicitudes del otro.

Artículo 62

Supervisión coordinada del Supervisor Europeo de Protección de Datos y las autoridades de control nacionales

1. Cuando un acto de la Unión haga referencia al presente artículo, el Supervisor Europeo de Protección de Datos y las autoridades de control nacionales, cada uno en el ámbito de sus competencias respectivas, cooperarán de forma activa en el marco de sus responsabilidades a fin de garantizar una supervisión efectiva de los sistemas informáticos a gran escala y de los órganos y organismos de la Unión.

2. En sus respectivos ámbitos de competencia y, en la medida necesaria, actuando cada uno en el marco de sus responsabilidades, intercambiarán la información oportuna, se prestarán mutuamente ayuda en el desarrollo de las auditorías e inspecciones, examinarán las dificultades de interpretación o aplicación del presente Reglamento y de otros actos de la Unión aplicables, estudiarán los problemas que plantee el ejercicio de una supervisión independiente o que surjan en el ejercicio de los derechos de los interesados, elaborarán propuestas armonizadas para aportar soluciones a cualquier problema existente y fomentarán el conocimiento de los derechos relacionados con la protección de dato.

3. A los fines establecidos en el apartado 2, el Supervisor Europeo de Protección de Datos y las autoridades de control nacionales se reunirán al menos dos veces al año en el marco del Comité Europeo de Protección de Datos. A tal fin, el Comité Europeo de Protección de Datos podrá desarrollar nuevos métodos de trabajo en función de las necesidades.

4. Cada dos años el Comité Europeo de Protección de Datos remitirá al Parlamento Europeo, al Consejo y a la Comisión un informe conjunto sobre las actividades relativas a la supervisión coordinada.

([1]) Decisión 2009/917/JAI del Consejo, de 30 de noviembre de 2009, sobre la utilización de la tecnología de la información a efectos aduaneros (DO L 323 de 10.12.2009, p. 20).

CAPÍTULO VIII

RECURSOS, RESPONSABILIDAD Y SANCIONES

Artículo 63

Derecho a presentar una reclamación ante el Supervisor Europeo de Protección de Datos

1. Sin perjuicio de los recursos judiciales, administrativos o extrajudiciales, todo interesado tendrá derecho a presentar una reclamación ante el Supervisor Europeo de Protección de Datos si considera que el tratamiento de sus datos personales infringe el presente Reglamento.

2. El Supervisor Europeo de Protección de Datos informará al reclamante del curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 64.

3. Si el Supervisor Europeo de Protección de Datos no da curso a la reclamación o no informa al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación, se entenderá que el Supervisor Europeo de Protección de Datos ha adoptado una decisión negativa.

Artículo 64

Derecho a la tutela judicial efectiva

1. El Tribunal de Justicia será competente en todos los litigios relativos a las disposiciones del presente Reglamento, incluidas las acciones de indemnización por daños y perjuicios.

2. Las decisiones del Supervisor Europeo de Protección de Datos, incluidas las decisiones a que se refiere el artículo 63, apartado 3, podrán recurrirse ante el Tribunal de Justicia.

3. El Tribunal de Justicia gozará de competencia jurisdiccional plena para revisar las multas administrativas a que se hace referencia en el artículo 66. Podrá anular, reducir o incrementar el importe de dichas multas, dentro de los límites del artículo 66.

Artículo 65

Derecho a indemnización

Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir de la institución u organismo de la Unión responsable una indemnización por los daños y perjuicios sufridos, con arreglo a las condiciones previstas en los Tratados.

Artículo 66

Multas administrativas

1. El Supervisor Europeo de Protección de Datos podrá imponer multas administrativas a las instituciones y organismos de la Unión, según las circunstancias de cada caso particular, cuando estas incumplan una de sus resoluciones con arreglo a lo dispuesto en el artículo 58, apartado 2, letras d) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) cualquier medida tomada por la institución u organismo de la Unión para paliar los daños y perjuicios sufridos por los interesados;

c) el grado de responsabilidad de la institución u organismo de la Unión, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 27 y 33;

d) toda infracción anterior similar cometida por la institución u organismo de la Unión;

e) el grado de cooperación con el Supervisor Europeo de Protección de Datos con el fin de poner remedio a la infracción y mitigar sus posibles efectos adversos;

f) las categorías de los datos de carácter personal afectados por la infracción;

g) la forma en que el Supervisor Europeo de Protección de Datos tuvo conocimiento de la infracción, en particular si la institución u organismo de la Unión la notificó y, en tal caso, en qué medida;

h) el cumplimiento de cualquiera de las medidas indicadas en el artículo 58 que hayan sido ordenadas previamente contra la institución u organismo de la Unión de que se trate en relación con el mismo asunto. Los procedimientos que llevan a la imposición de dichas multas se llevarán a cabo en un plazo razonable según las circunstancias de cada caso y teniendo en cuenta las acciones pertinentes y los procedimientos mencionados en el artículo 69.

2. Las infracciones de las obligaciones de la institución u organismo de la Unión en virtud de los artículos 8, 12, 27 a 35, 39, 40, 43, 44 y 45 se sancionarán, de acuerdo con el apartado 1, con multas administrativas de hasta 25 000 EUR como máximo por cada infracción, hasta un total de 250 000 EUR al año.

3. Las infracciones de las disposiciones siguientes por parte de la institución u organismo de la Unión se sancionarán, de acuerdo con el apartado 1, con multas administrativas de hasta 50 000 EUR como máximo por cada infracción, hasta un total de 500 000 EUR al año:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 4, 5, 7 y 10;

b) los derechos de los interesados a tenor de los artículos 14 a 24;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 46 a 50.

4. Si una institución u organismo de la Unión incumpliera, para las mismas operaciones de tratamiento, operaciones vinculadas u operaciones continuas, diversas disposiciones del presente Reglamento o la misma disposición en varias ocasiones, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

5. Antes de tomar ninguna decisión en virtud de este artículo, el Supervisor Europeo de Protección de Datos ofrecerá a la institución u organismo de la Unión sometida al procedimiento instruido por el Supervisor Europeo de Protección de Datos la oportunidad de manifestar su opinión con respecto a los cargos que le sean imputados por este. El Supervisor Europeo de Protección de Datos basará sus decisiones únicamente en las objeciones sobre las que las partes afectadas hayan podido manifestarse. Los denunciantes participarán estrechamente en el procedimiento.

6. Los derechos de defensa de las partes estarán garantizados plenamente en el curso del procedimiento. Tendrán derecho a acceder al expediente del Supervisor Europeo de Protección de Datos, sin perjuicio del interés legítimo de las personas físicas y las empresas en la protección de sus datos personales o secretos comerciales.

7. La recaudación proveniente de la imposición de multas con arreglo al presente artículo pasará a engrosar los ingresos del presupuesto general de la Unión.

Artículo 67

Representación de los interesados

El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de la Unión o de un Estado miembro, cuyos objetivos legales sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación ante el Supervisor Europeo de Protección de Datos, y ejerza en su nombre los derechos recogidos en los artículos 63 y 64, y el derecho a ser indemnizado mencionado en el artículo 65.

Artículo 68

Reclamaciones del personal de la Unión

Toda persona empleada por una institución u organismo de la Unión podrá presentar una reclamación ante el Supervisor Europeo de Protección de Datos en caso de presunta infracción de las disposiciones del presente Reglamento, incluso sin necesidad de seguir los conductos oficiales. Nadie habrá de sufrir perjuicio alguno por haber presentado una reclamación ante el Supervisor Europeo de Protección de Datos en la que se denuncie tal infracción.

Artículo 69

Sanciones

En el supuesto de que un funcionario u otro agente de la Unión incumpla, ya sea intencionadamente o por negligencia, las obligaciones establecidas en el presente Reglamento, dicho funcionario u otro agente quedará sujeto a medidas disciplinarias o de otro tipo, de conformidad con las normas y procedimientos establecidos en el Estatuto de los funcionarios.

CAPÍTULO IX

TRATAMIENTO DE DATOS PERSONALES OPERATIVOS POR LOS ÓRGANOS Y ORGANISMOS DE LA UNIÓN CUANDO LLEVAN A CABO ACTIVIDADES COMPRENDIDAS EN EL ÁMBITO DE APLICACIÓN DE LOS CAPÍTULOS 4 O 5 DEL TÍTULO V DE LA TERCERA PARTE DEL TFUE

Artículo 70

Ámbito de aplicación del capítulo

El presente capítulo se aplicará exclusivamente al tratamiento de datos personales operativos por los órganos y organismos de la Unión cuando llevan a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE, sin perjuicio de las normas específicas en materia de protección de datos aplicables a dichos órganos u organismos de la Unión.

Artículo 71

Principios relativos al tratamiento de datos personales operativos

1. Los datos personales operativos serán:

a) tratados de manera lícita y leal («licitud y lealtad»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines («limitación de la finalidad»);

c) adecuados, pertinentes y no excesivos en relación con los fines para los que se traten («minimización de los datos»);

d) exactos y, si fuera necesario, actualizados; se tomarán todas las medidas razonables para la supresión o rectificación sin dilación de los datos personales que sean inexactos en relación con los fines para los que son tratados («exactitud»);

e) conservados de una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que son tratados («limitación de la conservación»);

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

2. Se permitirá el tratamiento de los datos personales operativos por el mismo responsable del tratamiento o por otro para cualquier fin establecido en el acto jurídico que establezca el órgano u organismo de la Unión, distinto del fin para el que se recojan dichos datos en la medida en que:

a) el responsable del tratamiento esté autorizado a tratar dichos datos personales operativos para ese fin de conformidad con el Derecho de la Unión; y

b) el tratamiento sea necesario y proporcionado para ese otro fin de conformidad con el Derecho de la Unión.

3. El tratamiento por el mismo responsable del tratamiento o por otro podrá incluir el archivo en el interés público, el uso científico, estadístico o histórico para los fines establecidos en el acto jurídico por el que se establezca el órgano u organismo de la Unión, con sujeción a las salvaguardias adecuadas para los derechos y libertades de los interesados.

4. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en los apartados 1, 2 y 3, y capaz de demostrarlo.

Artículo 72

Licitud del tratamiento de datos personales operativos

1. El tratamiento de datos personales operativos será lícito únicamente cuando, y en la medida en que, dicho tratamiento sea necesario para el ejercicio de una función efectuada por órganos y organismos de la Unión cuando llevan a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE y esté basado en el Derecho de la Unión.

2. Los actos jurídicos específicos de la Unión que regulen el tratamiento dentro del ámbito de aplicación del presente capítulo especificarán, como mínimo, los fines del tratamiento y los plazos de conservación de los datos personales operativos o para la revisión periódica de la necesidad de un nuevo almacenamiento de los datos personales operativos.

Artículo 73

Distinción entre diferentes categorías de interesados

Cuando corresponda, y en la medida de lo posible, el responsable del tratamiento hará una distinción clara entre los datos personales operativos de las distintas categorías de interesados, como por ejemplo las categorías mencionadas en los actos jurídicos por los que se establecen los órganos y organismos de la Unión.

Artículo 74

Distinción entre datos personales operativos y verificación de la calidad de los datos personales operativos

1. El responsable del tratamiento distinguirá, en la medida de lo posible, los datos personales operativos basados en hechos de los datos personales operativos basados en evaluaciones personales.

2. El responsable del tratamiento tomará todas las medidas razonables para garantizar que los datos personales operativos que sean inexactos, incompletos o que no estén actualizados no se transmitan ni se pongan a disposición. Para ello, el responsable del tratamiento verificará, en la medida en que sea factible y cuando sea pertinente, la calidad de los datos personales operativos antes de transmitirlos o ponerlos a disposición de terceros, por ejemplo consultando a la autoridad competente de la que proceden los datos. En la medida de lo posible, en todas las transmisiones de datos personales operativos, el responsable del tratamiento añadirá la información necesaria para que el destinatario pueda valorar en qué medida los datos personales operativos son exactos, completos y fiables, y en qué medida están actualizados.

3. Si se observara que se han transmitido datos personales operativos incorrectos o se han transmitido datos personales operativos ilícitamente, el hecho deberá ponerse en conocimiento del destinatario sin dilación. En tal caso, los datos personales operativos de que se trate deberán rectificarse o suprimirse, o su tratamiento deberá limitarse de conformidad con el artículo 82.

Artículo 75

Condiciones específicas de tratamiento

1. Cuando el Derecho de la Unión aplicable al responsable del tratamiento encargado de la transmisión establezca condiciones específicas para el tratamiento, el responsable del tratamiento informará de dichas condiciones y de la exigencia de cumplirlas al destinatario de dichos datos personales operativos.

2. El responsable del tratamiento cumplirá las condiciones específicas de tratamiento establecidas por la autoridad competente para la transmisión de conformidad con el artículo 9, apartados 3 y 4, de la Directiva (UE) 2016/680.

Artículo 76

Tratamiento de categorías especiales de datos personales operativos

1. El tratamiento de datos personales operativos 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 destinados a identificar de manera unívoca a una persona física, datos personales operativos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física solo se permitirá cuando sea estrictamente necesario por razones operativas, dentro del mandato del órgano u organismo de la Unión de que se trate y con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado. Estará prohibida la discriminación de personas físicas sobre la base de dichos datos.

2. Cuando se invoque el presente artículo se informará sin demora al delegado de protección de datos.

Artículo 77

Mecanismo de decisión individual automatizado, incluida la elaboración de perfiles

1. Estarán prohibidas 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 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 76, 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 76 quedará prohibida, de conformidad con el Derecho de la Unión.

Artículo 78

Comunicación y modalidades de ejercicio de los derechos de los interesados

1. El responsable del tratamiento adoptará medidas razonables para facilitar al interesado toda la información a que se refiere el artículo 79, así como cualquier comunicación a que se refieren los artículos 80 a 84 y 92 relativa al tratamiento, de 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 del tratamiento facilitará la información por un medio idéntico al utilizado para la solicitud.

2. El responsable del tratamiento deberá facilitar el ejercicio de los derechos de los interesados con arreglo a lo dispuesto en los artículos 79 a 84.

3. El responsable del tratamiento informará por escrito al interesado, sin dilación indebida, sobre el curso dado a su solicitud y en cualquier caso en un plazo de tres meses a partir de la recepción de la solicitud por el interesado.

4. El responsable del tratamiento dispondrá que la información facilitada con arreglo al artículo 79 y cualquier comunicación efectuada y acción realizada en virtud de los artículos 80 a 84 y 92 a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

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 80 u 82 podrá solicitar que se facilite la información complementaria necesaria para confirmar la identidad del interesado.

Artículo 79

Información que debe ponerse a disposición del interesado o que se le debe proporcionar

1. El responsable del tratamiento pondrá a disposición del interesado al menos la siguiente información:

a) la identidad y los datos de contacto del órgano u organismo de la Unión;

b) los datos de contacto del delegado de protección de datos;

c) los fines del tratamiento a que se destinen los datos personales operativos;

d) el derecho a presentar una reclamación ante el Supervisor Europeo de Protección de Datos y los datos de contacto de este;

e) la existencia del derecho a solicitar del responsable el acceso a los datos personales operativos 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, el responsable del tratamiento proporcionará al interesado, en los casos específicos previstos en el Derecho de la Unión, 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 operativos o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo;

c) cuando corresponda, las categorías de destinatarios de los datos personales operativos, en particular en terceros países u organizaciones internacionales;

d) cuando sea necesario, más información, en particular cuando los datos personales operativos se hayan recogido sin conocimiento del interesado.

3. El responsable del tratamiento podrá retrasar, limitar u omitir la puesta a disposición del interesado de la información en virtud del apartado 2 siempre y cuando una medida de esa naturaleza constituya una medida necesaria y proporcionada 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 de índole oficial o legal;

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 de los Estados miembros;

d) proteger la seguridad nacional de los Estados miembros;

e) proteger los derechos y libertades de otras personas, como las víctimas o los testigos.

Artículo 80

Derecho de acceso del interesado

El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, tendrá derecho a acceder a los datos personales operativos y a la información siguiente:

a) los fines y la base jurídica del tratamiento;

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

c) los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales operativos, en particular los destinatarios de terceros países u organizaciones internacionales;

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

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

f) el derecho a presentar una reclamación ante el Supervisor Europeo de Protección de Datos y sus datos de contacto;

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

Artículo 81

Limitaciones al derecho de acceso

1. El responsable del tratamiento podrá restringir, total o parcialmente, el derecho de acceso del interesado siempre y cuando dicha restricción parcial o completa constituya una medida necesaria y proporcionada 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 de índole oficial o legal;

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 de los Estados miembros;

d) proteger la seguridad nacional de los Estados miembros;

e) proteger los derechos y libertades de otras personas, como por ejemplo víctimas y testigos.

2. En los casos contemplados en el apartado 1, el responsable del tratamiento informará por escrito al interesado, sin demora injustificada, de cualquier denegación o limitación de acceso, y de las razones de la denegación o de la limitación. Esta información podrá omitirse cuando el suministro de dicha información pueda comprometer uno de los fines contemplados en el apartado 1. El responsable del tratamiento informará al interesado de la posibilidad de presentar una reclamación ante el Supervisor Europeo de Protección de Datos o de interponer recurso judicial ante el Tribunal de Justicia. El responsable del tratamiento documentará los fundamentos de hecho o de Derecho en los que se basa la decisión. Esta información se pondrá a disposición del Supervisor Europeo de Protección de Datos previa solicitud.

Artículo 82

Derecho de rectificación o supresión de datos personales operativos y limitación de su tratamiento

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

2. El responsable del tratamiento suprimirá los datos personales operativos sin dilación indebida, y el interesado tendrá derecho a obtener de él, sin dilación indebida, la supresión de los datos personales operativos que le conciernan cuando el tratamiento infrinja el artículo 71, el artículo 72, apartado 1, o el artículo 76, o cuando los datos personales operativos se supriman para dar cumplimiento a una obligación legal a la que esté sujeta al 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 su 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.

Los datos objeto de una limitación solo se tratarán para los fines que impidieron su supresión.

4. El responsable del tratamiento informará al interesado por escrito de cualquier denegación de rectificación o supresión de los datos personales operativos o de la limitación de su tratamiento, y de los motivos de la denegación. El responsable del tratamiento podrá limitar, total o parcialmente, la comunicación de tal información, siempre y cuando dicha limitación constituya una medida necesaria y proporcionada 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 de índole oficial o legal;

b) evitar que se cause perjuicio a la prevención, investigación, detección o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales;

c) proteger la seguridad pública de los Estados miembros;

d) proteger la seguridad nacional de los Estados miembros;

e) proteger los derechos y libertades de otras personas, como las víctimas o los testigos.

El responsable del tratamiento informará al interesado de la posibilidad de presentar una reclamación ante el Supervisor Europeo de Protección de Datos o de interponer recurso judicial ante el Tribunal de Justicia.

5. El responsable del tratamiento comunicará la rectificación de los datos personales operativos inexactos a la autoridad competente de la que procedan los datos personales operativos inexactos.

6. Cuando los datos personales operativos hayan sido rectificados o suprimidos o el tratamiento haya sido limitado en virtud de los apartados 1, 2 o 3, el responsable del tratamiento lo notificará a los destinatarios y les informará de su obligación de rectificar o suprimir los datos personales operativos que estén bajo su responsabilidad o de limitar su tratamiento.

Artículo 83

Derecho de acceso en las investigaciones y los procesos penales

Cuando los datos personales operativos procedan de una autoridad competente, los órganos y organismos de la Unión, antes de decidir sobre el derecho de acceso del interesado verificarán, junto con la autoridad competente interesada, si dichos datos personales figuran en una resolución judicial o en un registro o expediente tramitado en el curso de investigaciones y procesos penales en el Estado miembro de dicha autoridad competente. De ser el caso, se tomará una decisión sobre el derecho de acceso en consulta y estrecha cooperación con la autoridad competente de que se trate.

Artículo 84

Ejercicio de los derechos del interesado y comprobación por el Supervisor Europeo de Protección de Datos

1. En los casos a que se refieren el artículo 79, apartado 3, el artículo 81 y el artículo 82, apartado 4, los derechos del interesado también podrán ejercerse a través del Supervisor Europeo de Protección de Datos.

2. El responsable del tratamiento informará al interesado de la posibilidad de ejercer sus derechos a través del Supervisor Europeo de Protección de Datos con arreglo al apartado 1.

3. Cuando se ejerza el derecho a que se refiere el apartado 1, el Supervisor Europeo de Protección de Datos informará al interesado, al menos, de que ha efectuado todas las verificaciones necesarias o la revisión correspondiente. El Supervisor Europeo de Protección de Datos también informará al interesado de su derecho a interponer recurso ante el Tribunal de Justicia.

Artículo 85

Protección de datos desde el diseño y por defecto

1. El responsable del tratamiento, teniendo en cuenta los últimos adelantos de la técnica, el coste de la aplicación y la naturaleza, el alcance, 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, aplicará 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 del presente Reglamento y del acto jurídico que lo establece, y se protejan los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas adecuadas para garantizar que, por defecto, solo sean objeto de tratamiento los datos personales operativos que sean adecuados, pertinentes y no excesivos en relación con los fines de su tratamiento. Esta obligación se aplicará a la cantidad de datos personales operativos recogidos, a la extensión de su tratamiento, a su período de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

Artículo 86

Corresponsables del tratamiento

1. Cuando dos o más responsables del tratamiento o uno o más responsables junto con otro u otros responsables distintos de las instituciones y organismos de la Unión determinen conjuntamente los objetivos y medios del tratamiento, serán considerados corresponsables del tratamiento. Los corresponsables del tratamiento determinarán de modo transparente sus responsabilidades respectivas en el cumplimiento de sus obligaciones en materia de protección de datos, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de facilitar la información a que se refiere el artículo 79, mediante un acuerdo entre ellos, salvo que, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que les sea aplicable. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo mencionado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas que los corresponsables del tratamiento tengan respecto del interesado. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo mencionado en el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento con respecto a cada uno de los responsables del tratamiento y frente a ellos.

Artículo 87

Encargado del tratamiento

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

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

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

a) actúe únicamente siguiendo las instrucciones del responsable;

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

c) asista al responsable por cualquier medio adecuado para garantizar el cumplimiento de las disposiciones sobre los derechos del interesado;

d) a elección del responsable, suprima o devuelva a este todos los datos personales operativos una vez finalice la prestación de los servicios de tratamiento, y suprima las copias existentes a menos que se requiera la conservación de los datos personales operativos en virtud del Derecho de la Unión o de un Estado miembro;

e) ponga a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo;

f) respete los requisitos exigidos en el apartado 2 y en el presente apartado 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, al determinar los fines y medios del tratamiento, un encargado del tratamiento infringe el presente Reglamento o el acto jurídico por el que se establece el responsable del tratamiento, el encargado será considerado responsable del tratamiento con respecto a ese tratamiento.

Artículo 88

Registro de operaciones

1. El responsable del tratamiento conservará registros de cada una de las operaciones de tratamiento siguientes en sistemas de tratamiento automatizados: recogida, alteración, acceso, consulta, comunicación, incluidas las transferencias, combinación y supresión de datos personales operativos. Los registros de operaciones de consulta y comunicación harán posible determinar la justificación, así como la fecha y la hora, de tales operaciones y el nombre de la persona que consultó o comunicó datos personales operativos, así como, en la medida de lo posible, la identidad de los destinatarios de dichos datos personales operativos.

2. Dichos registros se utilizarán únicamente a efectos de verificar la licitud del tratamiento, de autocontrol, de garantizar la integridad y la seguridad de los datos personales operativos y en el ámbito de los procesos penales. Los registros se eliminarán transcurridos tres años, a menos que sean necesarios para efectuar un control continuo.

3. El responsable del tratamiento pondrá los registros a disposición del correspondiente delegado de protección de datos y del Supervisor Europeo de Protección de Datos previa petición.

Artículo 89

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, el responsable del tratamiento llevará a cabo, de forma previa, una evaluación de impacto de las operaciones de tratamiento previstas en la protección de datos personales operativos.

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 operativos y a demostrar la conformidad con las normas en materia de protección de datos, teniendo en cuenta los derechos e intereses legítimos de los interesados y las demás personas afectadas.

Artículo 90

Consulta previa al Supervisor Europeo de Protección de Datos

1. El responsable del tratamiento consultará al Supervisor Europeo de Protección de Datos antes de un tratamiento que vaya a formar parte de un nuevo sistema de archivo que haya de crearse, cuando:

a) la evaluación del impacto en la protección de los datos que dispone el artículo 89 indique que el tratamiento entrañaría un alto riesgo a falta de medidas adoptadas por el responsable del tratamiento para 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 las libertades de los interesados.

2. El Supervisor Europeo de Protección de Datos podrá establecer una lista de las operaciones de tratamiento que están sujetas a consulta previa con arreglo a lo dispuesto en el apartado 1.

3. El responsable del tratamiento facilitará al Supervisor Europeo de Protección de Datos la evaluación de impacto relativa a la protección de datos a que se refiere el artículo 89 y, previa solicitud, cualquier información adicional que permita al Supervisor Europeo de Protección de Datos evaluar la conformidad del tratamiento y, en particular, los riesgos para la protección de los datos personales operativos del interesado y las garantías correspondientes.

4. En los casos en que el Supervisor Europeo de Protección de Datos considere que el tratamiento previsto a que se refiere el apartado 1 contraviene lo dispuesto en el presente Reglamento o el acto jurídico por el que se establece el órgano u organismo de la Unión, especialmente en caso de que la este último tenga insuficientemente identificados o atenuados los riesgos, el Supervisor Europeo de Protección de Datos deberá proporcionar asesoramiento escrito al responsable del tratamiento, en un plazo máximo de seis semanas a partir de la recepción de la solicitud de consulta. Este plazo podrá prorrogarse un mes, en función de la complejidad del tratamiento previsto. El Supervisor Europeo de Protección de Datos informará al responsable del tratamiento 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.

Artículo 91

Seguridad del tratamiento de datos personales operativos

1. El responsable del tratamiento y el encargado del tratamiento, teniendo en cuenta los últimos adelantos de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como la probabilidad y gravedad de los distintos riesgos que plantee el tratamiento para los derechos y libertades de las personas físicas, aplicarán las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad que corresponda según los riesgos, en particular en lo que se refiere al tratamiento de categorías especiales de datos personales operativos.

2. En relación con el tratamiento automatizado, el responsable del tratamiento y el encargado del tratamiento, tras una evaluación de los riesgos, aplicarán medidas destinadas a:

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

b) impedir que los soportes de datos puedan ser leídos, copiados, modificados o cancelados sin autorización («control de los soportes de datos»);

c) impedir la introducción no autorizada de datos personales operativos y la inspección, modificación o supresión no autorizadas de datos personales operativos conservados («control de la conservación»);

d) impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de comunicación 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 operativos para los que han sido autorizadas («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 disposición de qué organismos pueden ponerse los datos personales operativos mediante la comunicación de datos («control de la transmisión»);

g) garantizar que pueda verificarse y comprobarse *a posteriori* qué datos personales operativos se han introducido en los sistemas de tratamiento automatizado de datos y en qué momento y por qué persona han sido introducidos («control de la introducción»);

h) impedir que, en el momento de la transmisión de datos personales operativos o durante el transporte de soportes de datos, los datos personales operativos 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 operativos almacenados no se degraden por fallos de funcionamiento del sistema («integridad»).

Artículo 92

Notificación al Supervisor Europeo de Protección de Datos de una violación de la seguridad de datos personales

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

2. La notificación del apartado 1 deberá, como mínimo:

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

b) comunicar el nombre y los datos de contacto del delegado de protección de datos;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

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

3. Si no fuera posible, o en la medida en que no sea posible, facilitar simultáneamente la información mencionada en el apartado 2, se podrá facilitar la información por etapas sin otra dilación indebida.

4. El responsable del tratamiento documentará cualquier violación de la seguridad de 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 permitirá al Supervisor Europeo de Protección de Datos verificar el cumplimiento de lo dispuesto en el presente artículo.

5. Cuando la violación de los datos personales operativos tenga que ver con datos que hayan sido transmitidos por o a las autoridades competentes, el responsable del tratamiento comunicará la información a que se refiere el apartado 2 a las autoridades competentes de que se trate sin dilación indebida.

Artículo 93

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

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

2. La comunicación al interesado indicada 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 recomendaciones a que se hace referencia en el artículo 92, apartado 2, letras b), c) y d).

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

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

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

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

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

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 indican en el artículo 79, apartado 3.

Artículo 94

Transferencia de datos personales operativos a terceros países y organizaciones internacionales

1. Conforme a las limitaciones y condiciones establecidas en los actos jurídicos por los que se establecen los órganos u organismos de la Unión, el responsable del tratamiento podrá transferir datos personales operativos a una autoridad de un tercer país o a una organización internacional en la medida en que esa transferencia sea necesaria para el desempeño de las tareas del responsable del tratamiento, y únicamente cuando se cumplan las condiciones establecidas en el presente artículo, en particular:

a) la Comisión haya adoptado una decisión de adecuación con arreglo al artículo 36, apartado 3, de la Directiva (UE) 2016/680, que acredite que el tercer país o un territorio o un sector de tratamiento de datos de ese tercer país, o la organización internacional de que se trate, garantizan un nivel de protección adecuado;

b) a falta de una decisión de la Comisión sobre la adecuación con arreglo a la letra a), la Comisión haya celebrado un acuerdo internacional entre la Unión y ese tercer país u organización internacional con arreglo al artículo 218 del TFUE que ofrezca garantías adecuadas con respecto a la protección de la intimidad y los derechos y libertades fundamentales de las personas físicas;

c) a falta de una decisión de la Comisión sobre la adecuación con arreglo a la letra a), o de un acuerdo internacional con arreglo a la letra b), se haya celebrado un acuerdo de cooperación que permita el intercambio de datos personales operativos antes de la fecha de aplicación del respectivo acto jurídico por el que se establece el órgano u organismo de la Unión de que se trate, entre ese órgano u organismo de la Unión y el tercer país en cuestión.

2. Los actos jurídicos por los que se establecen los órganos y organismos de la Unión podrán mantener o introducir disposiciones más específicas sobre las condiciones para las transferencias internacionales de datos personales operativos, en particular sobre las transferencias mediante salvaguardias y excepciones adecuadas para situaciones específicas.

3. El responsable del tratamiento publicará en su sitio web y mantendrá al día la lista de decisiones de adecuación a que se refiere el apartado 1, letra a), y de acuerdos, convenios administrativos y otros instrumentos relacionados con la transferencia de datos personales operativos de conformidad con el apartado 1.

4. El responsable del tratamiento llevará un registro pormenorizado de todas las transferencias realizadas de conformidad con el presente artículo.

Artículo 95

Confidencialidad de las medidas de investigación judicial y del proceso penal

Los actos jurídicos por los que se establecen los órganos u organismos de la Unión que lleven a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE podrán obligar al Supervisor Europeo de Protección de Datos, en el ejercicio de sus competencias de control, a tener lo más en cuenta posible la confidencialidad de las medidas de investigación judicial y del proceso penal, de conformidad con el Derecho de la Unión o de los Estados miembros.

CAPÍTULO X

ACTOS DE EJECUCIÓN

Artículo 96

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. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

CAPÍTULO XI

REVISIÓN

Artículo 97

Cláusula de revisión

A más tardar el 30 de abril de 2022, y posteriormente cada cinco años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la aplicación del presente Reglamento, acompañado, en su caso, de las propuestas legislativas oportunas.

Artículo 98

Revisión de actos jurídicos de la Unión

1. A más tardar el 30 de abril de 2022, la Comisión revisará los actos jurídicos adoptados sobre la base de los Tratados que regulan el tratamiento de datos personales operativos por parte de órganos u organismos de la Unión cuando llevan a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE, con el fin de:

a) evaluar su coherencia con la Directiva (UE) 2016/680 y el capítulo IX del presente Reglamento;

b) detectar las divergencias que puedan dificultar el intercambio de datos personales operativos entre los órganos u organismos de la Unión cuando llevan a cabo actividades en esos ámbitos y las autoridades competentes; y

c) detectar las divergencias que puedan dar lugar a una fragmentación jurídica de la legislación en materia de protección de datos en la Unión.

2. Sobre la base de la revisión, y a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento, la Comisión podrá presentar propuestas legislativas oportunas, en particular a efectos la aplicación del capítulo IX del presente Reglamento a Europol y a la Fiscalía Europea, incluyendo adaptaciones del capítulo IX del presente Reglamento, de ser necesario.

CAPÍTULO XII

DISPOSICIONES FINALES

Artículo 99

Derogación del Reglamento (CE) n.º 45/2001 y de la Decisión n.º 1247/2002/CE

Quedan derogados, con efectos a partir del 11 de diciembre de 2018, el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE. Las referencias al Reglamento y a la Decisión derogados se entenderán hechas al presente Reglamento.

Artículo 100

Medidas transitorias

1. La Decisión 2014/886/UE del Parlamento Europeo y del Consejo ([1]) y los actuales mandatos del Supervisor Europeo de Protección de Datos y el Supervisor Adjunto no se verán afectados por el presente Reglamento.

([1]) Decisión 2014/886/UE del Parlamento Europeo y del Consejo, de 4 de diciembre de 2014, por la que se nombra al Supervisor Europeo de Protección de Datos y al Supervisor Adjunto (DO L 351 de 9.12.2014, p. 9).

2. El Supervisor Adjunto recibirá la misma consideración que el secretario del Tribunal de Justicia en cuanto a la determinación de su salario, asignaciones, pensión de jubilación y demás ventajas de carácter retributivo.

3. El artículo 53, apartados 4, 5 y 7, y los artículos 55 y 56 del presente Reglamento se aplicarán al actual Supervisor Adjunto hasta el final de su mandato.

4. El Supervisor Adjunto asistirá al Supervisor Europeo de Protección de Datos en el cumplimiento de las funciones de este último y le sustituirá en caso de ausencia o impedimento hasta el final del mandato del actual Supervisor Adjunto.

Artículo 101

Entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. No obstante, el presente Reglamento se aplicará al tratamiento de datos personales por parte de Eurojust a partir del 12 de diciembre de 2019.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Estrasburgo, el 23 de octubre de 2018.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*La Presidenta*
A. TAJANI	K. EDTSTADLER