TEXTO OFICIAL DEL BOE

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

BOE-A-2018-16673
Última actualización en el BOE: 2026-10-08
Recopilado por Coposita el 2026-11-11

Cómo usar este PDF

- El índice dice en qué página empieza cada título y capítulo; pulsa una línea para ir allí. El panel lateral de tu lector tiene los mismos marcadores.
- Arriba, en cada página, ves en qué título y capítulo estás.
- Cada artículo va en su bloque, con la numeración destacada.
- El texto es el del BOE, sin alterar. Comprueba siempre la versión vigente en el BOE.

La citan: 71 programas de oposición de Coposita

Versión oficial: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Índice

PREÁMBULO · I 4

TÍTULO I 10

Disposiciones generales 10

TÍTULO II · Principios de protección de datos 11

TÍTULO III · Derechos de las personas 13

CAPÍTULO I · Transparencia e información 13

CAPÍTULO II · Ejercicio de los derechos 13

TÍTULO IV 16

Disposiciones aplicables a tratamientos concretos 16

TÍTULO V · Responsable y encargado del tratamiento 19

CAPÍTULO I 19

Disposiciones generales. Medidas de responsabilidad activa 19

CAPÍTULO II · Encargado del tratamiento 21

CAPÍTULO III · Delegado de protección de datos 22

CAPÍTULO IV · Códigos de conducta y certificación 24

TÍTULO VI · Transferencias internacionales de datos 25

TÍTULO VII · Autoridades de protección de datos 26

CAPÍTULO I · La Agencia Española de Protección de Datos 26

Sección 1.ª Disposiciones generales 26

Sección 2.ª Potestades de investigación y planes de auditoría preventiva 29

Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos 31

CAPÍTULO II · Autoridades autonómicas de protección de datos 33

Sección 1.ª Disposiciones generales 33

Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679 33

TÍTULO VIII · Procedimientos en caso de posible vulneración de la normativa de protección de datos 34

TÍTULO IX · Régimen sancionador 37

TÍTULO X · Garantía de los derechos digitales 43

Disposición adicional primera. Medidas de seguridad en el ámbito del sector público. 48

Disposición adicional segunda. Protección de datos y transparencia y acceso a la información pública. 49

Disposición adicional tercera. Cómputo de plazos. 49

Disposición adicional sexta. Incorporación de deudas a sistemas de información crediticia. 50

Disposición adicional octava. Potestad de verificación de las Administraciones Públicas. 51

Disposición adicional novena. Tratamiento de datos personales en relación con la notificación de incidentes de seguridad. 51

Disposición adicional décima. Comunicaciones de datos por los sujetos enumerados en el artículo 77.1. 51

Disposición adicional undécima. Privacidad en las comunicaciones electrónicas. 51

Disposición adicional duodécima. Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público. 51

Disposición adicional decimotercera. Transferencias internacionales de datos tributarios. 52

Disposición adicional decimocuarta. Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE. 52

Disposición adicional decimoquinta. Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores. 52

Disposición adicional decimosexta. Prácticas agresivas en materia de protección de datos. 52

Disposición adicional decimoséptima. Tratamientos de datos de salud. 53

Disposición adicional decimoctava. Criterios de seguridad. 54

Disposición adicional decimonovena. Derechos de los menores ante Internet. 54

Disposición adicional vigésima. Especialidades del régimen jurídico de la Agencia Española de Protección de Datos. 55

Disposición adicional vigésima primera. Educación digital. 55

Disposición adicional vigésima segunda. Acceso a los archivos públicos y eclesiásticos. 55

Disposición adicional vigésima tercera. Modelos de presentación de reclamaciones. 55

Disposición transitoria primera. Estatuto de la Agencia Española de Protección de Datos. 55

Disposición transitoria tercera. Régimen transitorio de los procedimientos. 56

Disposición transitoria cuarta. Tratamientos sometidos a la Directiva (UE) 2016/680. 56

Disposición transitoria quinta. Contratos de encargado del tratamiento. 56

Disposición derogatoria única. Derogación normativa. 56

Disposición final primera. Naturaleza de la presente ley. 57

Disposición final segunda. Título competencial. 57

Disposición final tercera. Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. 58

Disposición final cuarta. Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. 58

Disposición final quinta. Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad. 59

Disposición final sexta. Modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. 59

Disposición final séptima. Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. 60

Disposición final octava. Modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades. 61

Disposición final décima. Modificación de la Ley Orgánica 2/2006, de 3 de mayo, de Educación. 61

Disposición final decimotercera. Modificación del texto refundido de la Ley del Estatuto de los Trabajadores. 62

Disposición final decimocuarta. Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público. 62

Disposición final decimoquinta. Desarrollo normativo. 63

Disposición final decimosexta. Entrada en vigor. 63

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

PREÁMBULO

I

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva.

II

En los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. Así, se fueron adoptando en distintas instancias internacionales propuestas para la reforma del marco vigente. Y en este marco la Comisión lanzó el 4 de noviembre de 2010 su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», que constituye el germen de la posterior reforma del marco de la Unión Europea. Al propio tiempo, el Tribunal de Justicia de la Unión ha venido adoptando a lo largo de los últimos años una jurisprudencia que resulta fundamental en su interpretación.

El último hito en esta evolución tuvo lugar con la adopción del 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 sus 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), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales

o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

III

El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

Asimismo, se atiende a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, los retos planteados por la rápida evolución tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información. El carácter central de la información personal tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa. Procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios. Así, el Reglamento general de protección de datos contiene un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

En este punto hay que subrayar que no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico. En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia). Por último, los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea.

La adaptación al Reglamento general de protección de datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica.

IV

Internet, por otra parte, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. Ya en los años noventa, y conscientes del impacto que iba a producir Internet en nuestras vidas, los pioneros de la Red propusieron elaborar una Declaración de los Derechos del Hombre y del Ciudadano en Internet.

Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital de nuestra sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía.

Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.

V

Esta ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

El Título I, relativo a las disposiciones generales, comienza regulando el objeto de la ley orgánica, que es, conforme a lo que se ha indicado, doble. Así, en primer lugar, se pretende lograr la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento general de protección de datos, y completar sus disposiciones. A su vez, establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. Las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía. En segundo lugar, es también objeto de la ley garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Destaca la novedosa regulación de los datos referidos a las personas fallecidas, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido. También excluye del ámbito de aplicación los tratamientos que se rijan por disposiciones específicas, en referencia, entre otras, a la normativa que transponga la citada Directiva (UE) 2016/680, previéndose en la disposición transitoria cuarta la aplicación a estos tratamientos de la Ley Orgánica 15/1999, de 13 de diciembre, hasta que se apruebe la citada normativa.

En el Título II, «Principios de protección de datos», se establece que a efectos del Reglamento (UE) 2016/679 no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público. También se recoge expresamente el deber de confidencialidad, el tratamiento de datos amparado por la ley, las categorías especiales de datos y el tratamiento de datos de naturaleza penal, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como «consentimiento tácito», se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se mantiene en catorce años la edad a partir de la cual el menor puede prestar su consentimiento.

Se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal, Este es el caso, por ejemplo, de las bases de datos reguladas por ley y gestionadas por autoridades públicas que responden a objetivos específicos de control de riesgos y solvencia, supervisión e inspección del tipo de la Central de Información de Riesgos del Banco de España regulada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema

Financiero, o de los datos, documentos e informaciones de carácter reservado que obren en poder de la Dirección General de Seguros y Fondos de Pensiones de conformidad con lo previsto en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley. Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de «listas negras» de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la misma norma europea.

También en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

El Título III, dedicado a los derechos de las personas, adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Se hace uso en este Título de la habilitación permitida por el considerando 8 del Reglamento (UE) 2016/679 para complementar su régimen, garantizando la adecuada estructura sistemática del texto. A continuación, la ley orgánica contempla los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.

En el Título IV se recogen «Disposiciones aplicables a tratamientos concretos», incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de todos los tratamientos lícitos. Dentro de ellos cabe apreciar, en primer lugar, aquellos respecto de los que el legislador establece una presunción «iuris tantum» de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este Título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general. En todo caso, el hecho de que el legislador se refiera a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa establecidas en el Capítulo IV del reglamento europeo y en el Título V de esta ley orgánica.

El Título V se refiere al responsable y al encargado del tratamiento. Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan. Con el fin de aclarar estas novedades, la ley orgánica

mantiene la misma denominación del Capítulo IV del Reglamento, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las medidas generales de responsabilidad activa, al régimen del encargado del tratamiento, a la figura del delegado de protección de datos y a los mecanismos de autorregulación y certificación. La figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

El Título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El Título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la ley orgánica regula el régimen de la Agencia Española de Protección de Datos y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

El Título VIII regula el «Procedimientos en caso de posible vulneración de la normativa de protección de datos». El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de «ventanilla única» en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

La regulación se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos; y el plazo de tramitación de los procedimientos y, en su caso, su suspensión. Las especialidades del procedimiento se remiten al desarrollo reglamentario.

El Título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la ley orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el reglamento europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del Reglamento general de protección de datos.

El Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones. La ley orgánica aprovecha la cláusula residual del artículo 83.2 de la norma europea, referida a los factores agravantes o atenuantes, para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos.

Finalmente, el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Las disposiciones adicionales se refieren a cuestiones como las medidas de seguridad en el ámbito del sector público, protección de datos y transparencia y acceso a la información pública, cómputo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a prácticas abusivas que pudieran desarrollar ciertos operadores, o los tratamientos de datos de salud, entre otras.

De conformidad con la disposición adicional decimocuarta, la normativa relativa a las excepciones y limitaciones en el ejercicio de los derechos que hubiese entrado en vigor con anterioridad a la fecha de aplicación del reglamento europeo y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, seguirá vigente en tanto no sea expresamente modificada, sustituida o derogada. La pervivencia de esta normativa supone la continuidad de las excepciones y limitaciones que en ella se contienen hasta que se produzca su reforma o abrogación, si bien referida a los derechos tal y como se regulan en el Reglamento (UE) 2016/679 y en esta ley orgánica. Así, por ejemplo, en virtud de la referida disposición adicional, las Administraciones tributarias responsables de los ficheros de datos con

trascendencia tributaria a que se refiere el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, podrán, en relación con dichos datos, denegar el ejercicio de los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Las disposiciones transitorias están dedicadas, entre otras cuestiones, al estatuto de la Agencia Española de Protección de Datos, el régimen transitorio de los procedimientos o los tratamientos sometidos a la Directiva (UE) 2016/680. Se recoge una disposición derogatoria y, a continuación, figuran las disposiciones finales sobre los preceptos con carácter de ley ordinaria, el título competencial y la entrada en vigor.

Asimismo, se introducen las modificaciones necesarias de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, la Ley 14/1986, de 25 de abril, General de Sanidad, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Finalmente, y en relación con la garantía de los derechos digitales, también se introducen modificaciones en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, así como en el Texto Refundido de la Ley del Estatuto de los Trabajadores y en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.

TÍTULO I

Disposiciones generales

Artículo 1 Objeto de la ley.

La presente ley orgánica tiene por objeto:

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

Artículo 2 Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94.

1. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. Esta ley orgánica no será de aplicación:

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.

c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

3. Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

4. El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

5. El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables.

Se añade el apartado 5 por la disposición final 4.1 de la Ley Orgánica 7/2021, de 26 de mayo. Ref. BOE-A-2021-8806#df-4

Artículo 3 Datos de las personas fallecidas.

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

TÍTULO II

Principios de protección de datos

Artículo 4 Exactitud de los datos.

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del afectado.

b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.

c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.

d) Fuesen obtenidos de un registro público por el responsable.

Artículo 5 Deber de confidencialidad.

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Artículo 6 Tratamiento basado en el consentimiento del afectado.

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

Artículo 7 Consentimiento de los menores de edad.

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Artículo 8 Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Artículo 9 Categorías especiales de datos.

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Artículo 10 Tratamiento de datos de naturaleza penal.

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO III

Derechos de las personas

CAPÍTULO I · Transparencia e información

Artículo 11 Transparencia e información al afectado.

1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.

b) La finalidad del tratamiento.

c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En estos supuestos, la información básica incluirá también:

a) Las categorías de datos objeto de tratamiento.

b) Las fuentes de las que procedieran los datos.

CAPÍTULO II · Ejercicio de los derechos

Artículo 12 Disposiciones generales sobre ejercicio de los derechos.

1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.

6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

Artículo 13 Derecho de acceso.

1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

Artículo 14 Derecho de rectificación.

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Artículo 15 Derecho de supresión.

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Artículo 16 Derecho a la limitación del tratamiento.

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.

2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Artículo 17 Derecho a la portabilidad.

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

Artículo 18 Derecho de oposición.

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

TÍTULO IV

Disposiciones aplicables a tratamientos concretos

Artículo 19 Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

Artículo 20 Sistemas de información crediticia.

1. Salvo prueba en contrario, se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan los siguientes requisitos:

a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.

c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe.

La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.

d) Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

e) Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.

Cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud conforme a lo previsto en el artículo 18.1.a) del Reglamento (UE) 2016/679, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado.

f) Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

2. Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de corresponsables del tratamiento de los datos, siendo de aplicación lo establecido por el artículo 26 del Reglamento (UE) 2016/679.

Corresponderá al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.

3. La presunción a la que se refiere el apartado 1 de este artículo no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.

Artículo 21 Tratamientos relacionados con la realización de determinadas operaciones mercantiles.

1. Salvo prueba en contrario, se presumirán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.

2. En el caso de que la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo prevista en esta ley orgánica.

Artículo 22 Tratamientos con fines de videovigilancia.

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.

Artículo 23 Sistemas de exclusión publicitaria.

1. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

A tal efecto, podrán crearse sistemas de información, generales o sectoriales, por parte de las asociaciones y organismos a los que se refiere el apartado 2 del artículo 40 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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) que cuenten con una alta representatividad en los que solo se incluirán los datos imprescindibles para identificar a los afectados. Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas. Para la creación y mantenimiento de estos sistemas se observarán las medidas que se establezcan mediante desarrollo reglamentario.

2. Las entidades responsables de los sistemas de exclusión publicitaria comunicarán a la autoridad de control competente su creación, su carácter general o sectorial, así como el modo en que los afectados pueden incorporarse a los mismos y, en su caso, hacer valer sus preferencias.

La autoridad de control competente hará pública en su sede electrónica una relación de los sistemas de esta naturaleza que le fueran comunicados, incorporando la información mencionada en el párrafo anterior. A tal efecto, la autoridad de control competente a la que se haya comunicado la creación del sistema lo pondrá en conocimiento de las restantes autoridades de control para su publicación por todas ellas.

3. Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, este deberá informarle de los sistemas de exclusión publicitaria existentes, pudiendo remitirse a la información publicada por la autoridad de control competente.

4. Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo. A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente.

No será necesario realizar la consulta a la que se refiere el párrafo anterior cuando el afectado hubiera prestado, conforme a lo dispuesto en esta ley orgánica, su consentimiento para recibir la comunicación a quien pretenda realizarla.

Se modifica el apartado 1 por la disposición final 4 de la Ley 10/2025, de 26 de diciembre. Ref. BOE-A-2025-26698#df-4

Artículo 24 Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas.

Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas.

Dichos tratamientos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en esta ley orgánica y en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Se modifica por la disposición final 7 de la Ley 2/2023, de 20 de febrero. Ref. BOE-A-2023-4513#df-7

Artículo 25 Tratamiento de datos en el ámbito de la función estadística pública.

1. El tratamiento de datos personales llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica, así como en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

2. La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos en que la estadística para la que se requiera la información venga exigida por una norma de Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.

De conformidad con lo dispuesto en el artículo 11.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.

3. Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica.

Artículo 26 Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Pública

Será lícito el tratamiento por las Administraciones Públicas de datos con fines de archivo en interés público, que se someterá a lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica con las especialidades que se derivan de lo previsto en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, así como la legislación autonómica que resulte de aplicación.

Artículo 27 Tratamiento de datos relativos a infracciones y sanciones administrativas.

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO V

Responsable y encargado del tratamiento

CAPÍTULO I

Disposiciones generales. Medidas de responsabilidad activa

Artículo 28 Obligaciones generales del responsable y encargado del tratamiento.

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones 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, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Artículo 29 Supuestos de corresponsabilidad en el tratamiento.

La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Artículo 30 Representantes de los responsables o encargados del tratamiento no establecidos en la Unión Europea

1. En los supuestos en que el Reglamento (UE) 2016/679 sea aplicable a un responsable o encargado del tratamiento no establecido en la Unión Europea en virtud de lo dispuesto en su artículo 3.2 y el tratamiento se refiera a afectados que se hallen en España, la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos podrán imponer al representante, solidariamente con el responsable o encargado del tratamiento, las medidas establecidas en el Reglamento (UE) 2016/679.

Dicha exigencia se entenderá sin perjuicio de la responsabilidad que pudiera en su caso corresponder al responsable o al encargado del tratamiento y del ejercicio por el representante de la acción de repetición frente a quien proceda.

2. Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.

Artículo 31 Registro de las actividades de tratamiento.

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

Artículo 32 Bloqueo de los datos.

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

CAPÍTULO II · Encargado del tratamiento

Artículo 33 Encargado del tratamiento.

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

CAPÍTULO III · Delegado de protección de datos

Artículo 34 Designación de un delegado de protección de datos.

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Artículo 35 Cualificación del delegado de protección de datos.

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Artículo 36 Posición del delegado de protección de datos.

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Artículo 37 Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protecc de datos.

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

CAPÍTULO IV · Códigos de conducta y certificación

Artículo 38 Códigos de conducta.

1. Los códigos de conducta regulados por la sección 5.ª del Capítulo IV del Reglamento (UE) 2016/679 serán vinculantes para quienes se adhieran a los mismos.

Dichos códigos podrán dotarse de mecanismos de resolución extrajudicial de conflictos.

2. Dichos códigos podrán promoverse, además de por las asociaciones y organismos a los que se refiere el artículo 40.2 del Reglamento (UE) 2016/679, por empresas o grupos de empresas así como por los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica.

Asimismo, podrán ser promovidos por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del Reglamento (UE) 2016/679.

Los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado en la reclamación, sin perjuicio de lo dispuesto en el artículo 37 de esta ley orgánica. Además, sin menoscabo de las competencias atribuidas por el Reglamento (UE) 2016/679 a las autoridades de protección de datos, podrán voluntariamente y antes de llevar a cabo el tratamiento, someter al citado organismo o entidad de supervisión la verificación de la conformidad del mismo con las materias sujetas al código de conducta.

En caso de que el organismo o entidad de supervisión rechace o desestime la reclamación, o si el responsable o encargado del tratamiento no somete la reclamación a su decisión, el afectado podrá formularla ante la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos.

La autoridad de protección de datos competente verificará que los organismos o entidades que promuevan los códigos de conducta han dotado a estos códigos de organismos de supervisión que reúnan los requisitos establecidos en el artículo 41.2 del Reglamento (UE) 2016/679.

3. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente.

4. La Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos someterán los proyectos de código al mecanismo de coherencia mencionado en el artículo 63 de Reglamento (UE) 2016/679 en los supuestos en que ello proceda según su artículo 40.7. El procedimiento quedará suspendido en tanto el Comité Europeo de Protección de Datos no emita el dictamen al que se refieren los artículos 64.1.b) y 65.1.c) del citado reglamento.

Cuando sea una autoridad autonómica de protección de datos la que someta el proyecto de código al mecanismo de coherencia, se estará a lo dispuesto en el artículo 60 de esta ley orgánica.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos conforme al artículo 40.11 del citado reglamento.

El registro será accesible a través de medios electrónicos.

6. Mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.

Artículo 39 Acreditación de instituciones de certificación.

Sin perjuicio de las funciones y poderes de acreditación de la autoridad de control competente en virtud de los artículos 57 y 58 del Reglamento (UE) 2016/679, la acreditación de las instituciones de certificación a las que se refiere el artículo 43.1 del citado reglamento podrá ser llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

TÍTULO VI

Transferencias internacionales de datos

Artículo 40 Régimen de las transferencias internacionales de datos.

Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias.

En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.

Artículo 41 Supuestos de adopción por la Agencia Española de Protección de Datos.

1. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del citado reglamento.

2. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.

El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, y continuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente.

Artículo 42 Supuestos sometidos a autorización previa de las autoridades de protección de datos.

1. Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse en los siguientes supuestos:

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

El procedimiento tendrá una duración máxima de seis meses.

2. La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refieren los artículos 64.1.e), 64.1.f) y 65.1.c) del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia Española de Protección de Datos o, por conducto de la misma, a la autoridad de control competente, en su caso.

Artículo 43 Supuestos sometidos a información previa a la autoridad de protección de datos competente.

Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos.

Esta información deberá facilitarse con carácter previo a la realización de la transferencia.

Lo dispuesto en este artículo no será de aplicación a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos, de acuerdo con el artículo 49.3 del Reglamento (UE) 2016/679.

TÍTULO VII

Autoridades de protección de datos

CAPÍTULO I · La Agencia Española de Protección de Datos

Sección 1.ª Disposiciones generales

Artículo 44 Disposiciones generales.

1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Se relaciona con el Gobierno a través del Ministerio de Justicia.

2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.

3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

Se modifica el apartado 3 por la disposición final 4.2 de la Ley Orgánica 7/2021, de 26 de mayo. Ref. BOE-A-2021-8806#df-4

Artículo 45 Régimen jurídico.

1. La Agencia Española de Protección de Datos se rige por lo dispuesto en el Reglamento (UE) 2016/679, la presente ley orgánica y sus disposiciones de desarrollo.

Supletoriamente, en cuanto sea compatible con su plena independencia y sin perjuicio de lo previsto en el artículo 63.2 de esta ley orgánica, se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto mediante real decreto.

Artículo 46 Régimen económico presupuestario y de personal.

1. La Agencia Española de Protección de Datos elaborará y aprobará su presupuesto y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado.

2. El régimen de modificaciones y de vinculación de los créditos de su presupuesto será el establecido en el Estatuto de la Agencia Española de Protección de Datos.

Corresponde a la Presidencia de la Agencia Española de Protección de Datos autorizar las modificaciones presupuestarias que impliquen hasta un tres por ciento de la cifra inicial de su presupuesto total de gastos, siempre que no se incrementen los créditos para gastos de personal. Las restantes modificaciones que no excedan de un cinco por ciento del presupuesto serán autorizadas por el Ministerio de Hacienda y, en los demás casos, por el Gobierno.

3. La Agencia Española de Protección de Datos contará para el cumplimiento de sus fines con las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado, los bienes y valores que constituyan su patrimonio y los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidos en el artículo 58 del Reglamento (UE) 2016/679.

4. El resultado positivo de sus ingresos se destinará por la Agencia Española de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia.

5. El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral y se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normativa reguladora de los funcionarios públicos y, en su caso, por la normativa laboral.

6. La Agencia Española de Protección Datos elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto. En dicha relación de puestos de trabajo constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas.

7. Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, la gestión económico-financiera de la Agencia Española de Protección de Datos estará sometida al control de la Intervención General de la Administración del Estado en los términos que establece la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Artículo 47 Funciones y potestades de la Agencia Española de Protección de Datos.

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Artículo 48 La Presidencia de la Agencia Española de Protección de Datos.

1. La Presidencia de la Agencia Española de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

2. La Presidencia de la Agencia Española de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones, a excepción de las relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado.

En los supuestos de ausencia, vacante o enfermedad de la persona titular de la Presidencia o cuando concurran en ella alguno de los motivos de abstención o recusación previstos en el artículo 23 de la Ley 40/2015, de 1 de octubre, de

Régimen Jurídico del Sector Público, el ejercicio de las competencias relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica serán asumidas por la persona titular del órgano directivo que desarrolle las funciones de inspección. En el supuesto de que cualquiera de las circunstancias mencionadas concurriera igualmente en dicha persona, el ejercicio de las competencias afectadas será asumido por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

El ejercicio del resto de competencias será asumido por el Adjunto en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos y, en su defecto, por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

3. La Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

4. La Presidencia y el Adjunto de la Agencia Española de Protección de Datos serán nombrados por el Consejo de Ministros mediante real decreto.

5. El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de cinco años y puede ser renovado para otro período de igual duración.

La Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por:

a) Incumplimiento grave de sus obligaciones,

b) incapacidad sobrevenida para el ejercicio de su función,

c) incompatibilidad, o

d) condena firme por delito doloso.

En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas en el apartado 3 de este artículo.

6. Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

Se modifica el apartado 2 por la disposición final 9.1 de la Ley 11/2023, de 8 de mayo. Ref. BOE-A-2023-11022#df-9

Artículo 49 Consejo Consultivo de la Agencia Española de Protección de Datos.

1. La Presidencia de la Agencia Española de Protección de Datos estará asesorada por un Consejo Consultivo compuesto por los siguientes miembros:

a) Un Diputado, propuesto por el Congreso de los Diputados.

b) Un Senador, propuesto por el Senado.

c) Un representante designado por el Consejo General del Poder Judicial.

d) Un representante de la Administración General del Estado con experiencia en la materia, propuesto por el Ministro de Justicia.

e) Un representante de cada Comunidad Autónoma que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma.

f) Un experto propuesto por la Federación Española de Municipios y Provincias.

g) Un experto propuesto por el Consejo de Consumidores y Usuarios.

h) Dos expertos propuestos por las Organizaciones Empresariales.

i) Un representante de los profesionales de la protección de datos y de la privacidad, propuesto por la asociación de ámbito estatal con mayor número de asociados.

j) Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos previstos en el Capítulo IV del Título V, propuesto por el Ministro de Justicia.

k) Un experto, propuesto por la Conferencia de Rectores de las Universidades Españolas.

l) Un representante de las organizaciones que agrupan a los Consejos Generales, Superiores y Colegios Profesionales de ámbito estatal de las diferentes profesiones colegiadas, propuesto por el Ministro de Justicia.

m) Un representante de los profesionales de la seguridad de la información, propuesto por la asociación de ámbito estatal con mayor número de asociados.

n) Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno.

ñ) Dos expertos propuestos por las organizaciones sindicales más representativas.

2. A los efectos del apartado anterior, la condición de experto requerirá acreditar conocimientos especializados en el Derecho y la práctica en materia de protección de datos mediante el ejercicio profesional o académico.

3. Los miembros del Consejo Consultivo serán nombrados por orden del Ministro de Justicia, publicada en el Boletín Oficial del Estado.

4. El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al semestre.

5. Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante.

6. En todo lo no previsto por esta ley orgánica, el régimen, competencias y funcionamiento del Consejo Consultivo serán los establecidos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Artículo 50 Publicidad.

La Agencia Española de Protección de Datos publicará las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, las que pongan fin a los procedimientos sancionadores y a los procedimientos de apercibimiento, las que archiven las actuaciones previas de investigación, las dictadas respecto de las entidades a que se refiere el artículo 77.1 de esta ley orgánica, las que impongan medidas cautelares y las demás que disponga su Estatuto.

Se modifica por la disposición final 9.2 de la Ley 11/2023, de 8 de mayo. Ref. BOE-A-2023-11022#df-9

Sección 2.ª Potestades de investigación y planes de auditoría preventiva

Artículo 51 Ámbito y personal competente.

1. La Agencia Española de Protección de Datos desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII y de los planes de auditoría preventivas.

2. La actividad de investigación se llevará a cabo por los funcionarios de la Agencia Española de Protección de Datos o por funcionarios ajenos a ella habilitados expresamente por su Presidencia.

3. En los casos de actuaciones conjuntas de investigación conforme a lo dispuesto en el artículo 62 del Reglamento (UE) 2016/679, el personal de las autoridades de control de otros Estados Miembros de Unión Europea que colabore con la Agencia Española de Protección de Datos ejercerá sus facultades con arreglo a lo previsto en la presente ley orgánica y bajo la orientación y en presencia del personal de esta.

4. Los funcionarios que desarrollen actividades de investigación tendrán la consideración de agentes de la autoridad en el ejercicio de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio, incluso después de haber cesado en él.

Artículo 52 Deber de colaboración.

1. Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación.

Cuando la información contenga datos personales la comunicación de dichos datos estará amparada por lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679.

2. En el marco de las actuaciones previas de investigación, cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, las informaciones y datos que resulten imprescindibles con la exclusiva finalidad de lograr la identificación de los responsables de las conductas que pudieran ser constitutivas de infracción del Reglamento (UE) 2016/679 y de la presente ley orgánica.

En el supuesto de las Administraciones tributarias y de la Seguridad Social, la información se limitará a la que resulte necesaria para poder identificar inequívocamente contra quién debe dirigirse la actuación de la Agencia Española de Protección de Datos en los supuestos de creación de entramados societarios que dificultasen el conocimiento directo del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica.

3. Cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información los datos que obren en su poder y que resulten imprescindibles para la identificación del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica cuando se hubiere llevado a cabo mediante la utilización de un servicio de la sociedad de la información o la realización de una comunicación electrónica. A tales efectos, los datos que la Agencia Española de Protección de Datos podrá recabar al amparo de este apartado son los siguientes:

a) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de telefonía fija o móvil:

1.º El número de teléfono de origen de la llamada en caso de que el mismo se hubiese ocultado.

2.º El nombre, número de documento identificativo y dirección del abonado o usuario registrado al que corresponda ese número de teléfono.

3.º La mera confirmación de que se ha realizado una llamada específica entre dos números en una determinada fecha y hora.

b) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de la sociedad de la información:

1.º La identificación de la dirección de protocolo de Internet desde la que se hubiera llevado a cabo la conducta y la fecha y hora de su realización.

2.º Si la conducta se hubiese llevado a cabo mediante correo electrónico, la identificación de la dirección de protocolo de Internet desde la que se creó la cuenta de correo y la fecha y hora en que la misma fue creada.

3.º El nombre, número de documento identificativo y dirección del abonado o del usuario registrado al que se le hubiera asignado la dirección de Protocolo de Internet a la que se refieren los dos párrafos anteriores.

Estos datos deberán ser cedidos, previo requerimiento motivado de la Agencia Española de Protección de Datos, exclusivamente en el marco de actuaciones de investigación iniciadas como consecuencia de una denuncia presentada por un afectado respecto de una conducta de una persona jurídica o respecto a la utilización de sistemas que permitan la divulgación sin restricciones de datos personales. En el resto de los supuestos la cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales cuando resultara exigible.

Quedan excluidos de lo previsto en este apartado los datos de tráfico que los operadores estuviesen tratando con la exclusiva finalidad de dar cumplimiento a las obligaciones previstas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuya cesión solamente podrá tener lugar de acuerdo con lo dispuesto en ella, previa autorización judicial solicitada por alguno de los agentes facultados a los que se refiere el artículo 6 de dicha ley.

Artículo 53 Alcance de la actividad de investigación.

1. Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos necesarios, examinarlos en el lugar en que se encuentren depositados o en donde se lleven a cabo los tratamientos, obtener copia de ellos, inspeccionar los equipos físicos y lógicos y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación.

2. Cuando fuese necesario el acceso por el personal que desarrolla la actividad de investigación al domicilio constitucionalmente protegido del inspeccionado, será preciso contar con su consentimiento o haber obtenido la correspondiente autorización judicial.

3. Cuando se trate de órganos judiciales u oficinas judiciales el ejercicio de las facultades de inspección se efectuará a través y por mediación del Consejo General del Poder Judicial.

Artículo 53 bis. Actuaciones de investigación a través de sistemas digitales.

Las actuaciones de investigación podrán realizarse a través de sistemas digitales que, mediante la videoconferencia u otro sistema similar, permitan la comunicación bidireccional y simultánea de imagen y sonido, la interacción visual, auditiva y verbal entre la Agencia Española de Protección de Datos y el inspeccionado. Además, deben garantizar la transmisión y recepción seguras de los documentos e información que se intercambien, y, en su caso, recoger las evidencias necesarias y el resultado de las actuaciones realizadas asegurando su autoría, autenticidad e integridad.

La utilización de estos sistemas se producirá cuando lo determine la Agencia y requerirá la conformidad del inspeccionado en relación con su uso y con la fecha y hora de su desarrollo.

Se añade por la disposición final 9.3 de la Ley 11/2023, de 8 de mayo. Ref. BOE-A-2023-11022#df-9

Artículo 54 Planes de auditoría.

1. La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones del Reglamento (UE) 2016/679 y de la presente ley orgánica, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.

2. A resultas de los planes de auditoría, la Presidencia de la Agencia Española de Protección de Datos podrá dictar las directrices generales o específicas para un concreto responsable o encargado de los tratamientos precisas para asegurar la plena adaptación del sector o responsable al Reglamento (UE) 2016/679 y a la presente ley orgánica.

En la elaboración de dichas directrices la Presidencia de la Agencia Española de Protección de Datos podrá solicitar la colaboración de los organismos de supervisión de los códigos de conducta y de resolución extrajudicial de conflictos, si los hubiere.

3. Las directrices serán de obligado cumplimiento para el sector o responsable al que se refiera el plan de auditoría.

Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos

Artículo 55 Potestades de regulación. Circulares de la Agencia Española de Protección de Datos.

1. La Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, que se denominarán «Circulares de la Agencia Española de Protección de Datos».

2. Su elaboración se sujetará al procedimiento establecido en el Estatuto de la Agencia Española de Protección de Datos, que deberá prever los informes técnicos y jurídicos que fueran necesarios y la audiencia a los interesados.

3. Las circulares serán obligatorias una vez publicadas en el Boletín Oficial del Estado.

Artículo 56 Acción exterior.

1. Corresponde a la Agencia Española de Protección de Datos la titularidad y el ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos.

Asimismo a las comunidades autónomas, a través de las autoridades autonómicas de protección de datos, les compete ejercitar las funciones como sujetos de la acción exterior en el marco de sus competencias de conformidad con lo dispuesto en la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado, así como celebrar acuerdos internacionales administrativos en ejecución y concreción de un tratado internacional y acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, no vinculantes jurídicamente para quienes los suscriben, sobre materias de su competencia en el marco de la Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales.

2. La Agencia Española de Protección de Datos es el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier Convenio Internacional en el que sea parte el Reino de España que atribuya a una autoridad nacional de control esa competencia y la representante común de las autoridades de Protección de Datos en el Comité Europeo de Protección de Datos, conforme a lo dispuesto en el artículo 68.4 del Reglamento (UE) 2016/679.

La Agencia Española de Protección de Datos informará a las autoridades autonómicas de protección de datos acerca de las decisiones adoptadas en el Comité Europeo de Protección de Datos y recabará su parecer cuando se trate de materias de su competencia.

3. Sin perjuicio de lo dispuesto en el apartado 1, la Agencia Española de Protección de Datos:

a) Participará en reuniones y foros internacionales de ámbito distinto al de la Unión Europea establecidos de común acuerdo por las autoridades de control independientes en materia de protección de datos.

b) Participará, como autoridad española, en las organizaciones internacionales competentes en materia de protección de datos, en los comités o grupos de trabajo, de estudio y de colaboración de organizaciones internacionales que traten materias que afecten al derecho fundamental a la protección de datos personales y en otros foros o grupos de trabajo internacionales, en el marco de la acción exterior del Estado.

c) Colaborará con autoridades, instituciones, organismos y Administraciones de otros Estados a fin de impulsar, promover y desarrollar el derecho fundamental a la protección de datos, en particular en el ámbito iberoamericano, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia.

CAPÍTULO II · Autoridades autonómicas de protección de datos

Sección 1.ª Disposiciones generales

Artículo 57 Autoridades autonómicas de protección de datos.

1. Las autoridades autonómicas de protección de datos personales podrán ejercer, las funciones y potestades establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679, de acuerdo con la normativa autonómica, cuando se refieran a:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

2. Las autoridades autonómicas de protección de datos podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para la Agencia Española de Protección de Datos en el artículo 55 de esta ley orgánica.

Artículo 58 Cooperación institucional.

La Presidencia de la Agencia Española de Protección de Datos convocará, por iniciativa propia o cuando lo solicite otra autoridad, a las autoridades autonómicas de protección de datos para contribuir a la aplicación coherente del Reglamento (UE) 2016/679 y de la presente ley orgánica. En todo caso, se celebrarán reuniones semestrales de cooperación.

La Presidencia de la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán solicitar y deberán intercambiarse mutuamente la información necesaria para el cumplimiento de sus funciones y, en particular, la relativa a la actividad del Comité Europeo de Protección de Datos. Asimismo, podrán constituir grupos de trabajo para tratar asuntos específicos de interés común.

Artículo 59 Tratamientos contrarios al Reglamento (UE) 2016/679.

Cuando la Presidencia de la Agencia Española de Protección de Datos considere que un tratamiento llevado a cabo en materias que fueran competencia de las autoridades autonómicas de protección de datos vulnera el Reglamento (UE) 2016/679 podrá requerirlas a que adopten, en el plazo de un mes, las medidas necesarias para su cesación.

Si la autoridad autonómica no atendiere en plazo el requerimiento o las medidas adoptadas no supusiesen la cesación en el tratamiento ilícito, la Agencia Española de Protección de Datos podrá ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.

Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679

Artículo 60 Coordinación en caso de emisión de dictamen por el Comité Europeo de Protección de Datos.

Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando éstas, como autoridades competentes, deban someter su proyecto de decisión al citado comité o le soliciten el examen de un asunto en virtud de lo establecido en los apartados 1 y 2 del artículo 64 del Reglamento (UE) 2016/679.

En estos casos, la Agencia Española de Protección de Datos será asistida por un representante de la Autoridad autonómica en su intervención ante el Comité.

Artículo 61 Intervención en caso de tratamientos transfronterizos.

1. Las autoridades autonómicas de protección de datos ostentarán la condición de autoridad de control principal o interesada en el procedimiento establecido por el artículo 60 del Reglamento (UE) 2016/679 cuando se refiera a un tratamiento previsto en el artículo 57 de esta ley orgánica que se llevara a cabo por un responsable o encargado del

tratamiento de los previstos en el artículo 56 del Reglamento (UE) 2016/679, salvo que desarrollase significativamente tratamientos de la misma naturaleza en el resto del territorio español.

2. Corresponderá en estos casos a las autoridades autonómicas intervenir en los procedimientos establecidos en el artículo 60 del Reglamento (UE) 2016/679, informando a la Agencia Española de Protección de Datos sobre su desarrollo en los supuestos en que deba aplicarse el mecanismo de coherencia.

Artículo 62 Coordinación en caso de resolución de conflictos por el Comité Europeo de Protección de Datos.

1. Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando estas, como autoridades principales, deban solicitar del citado Comité la emisión de una decisión vinculante según lo previsto en el artículo 65 del Reglamento (UE) 2016/679.

2. Las autoridades autonómicas de protección de datos que tengan la condición de autoridad interesada no principal en un procedimiento de los previstos en el artículo 65 del Reglamento (UE) 2016/679 informarán a la Agencia Española de Protección de Datos cuando el asunto sea remitido al Comité Europeo de Protección de Datos, facilitándole la documentación e información necesarias para su tramitación.

La Agencia Española de Protección de Datos será asistida por un representante de la autoridad autonómica interesada en su intervención ante el mencionado comité.

TÍTULO VIII

Procedimientos en caso de posible vulneración de la normativa de protección de datos

Artículo 63 Régimen jurídico.

1. Las disposiciones de este Título serán de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquella investigue la existencia de una posible infracción de lo dispuesto en el mencionado reglamento y en la presente ley orgánica.

2. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

3. El Gobierno regulará por real decreto los procedimientos que tramite la Agencia Española de Protección de Datos al amparo de este Título, asegurando en todo caso los derechos de defensa y audiencia de los interesados.

Artículo 64 Forma de iniciación del procedimiento y duración.

1. Cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se iniciará por acuerdo de admisión a trámite, que se adoptará conforme a lo establecido en el artículo 65 de esta ley orgánica.

En este caso el plazo para resolver el procedimiento será de seis meses a contar desde la fecha en que hubiera sido notificado al reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación.

2. Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la presente ley orgánica, se iniciará mediante acuerdo de inicio, adoptado por propia iniciativa o como consecuencia de reclamación, que le será notificado al interesado.

Si el procedimiento se fundase en una reclamación formulada ante la Agencia Española de Protección de Datos, con carácter previo, esta decidirá sobre su admisión a trámite, conforme a lo dispuesto en el artículo 65 de esta ley orgánica.

Admitida a trámite la reclamación, así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 67 de esta ley orgánica.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

3. Cuando así proceda en atención a la naturaleza de los hechos y teniendo debidamente en cuenta los criterios establecidos en el artículo 83.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Agencia Española de Protección de Datos, previa audiencia al responsable o encargado del tratamiento, podrá dirigir un apercibimiento, así como ordenar al responsable o encargado del tratamiento que adopten las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos de una determinada manera y dentro del plazo especificado.

El procedimiento tendrá una duración máxima de seis meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

Será de aplicación en este caso lo dispuesto en los párrafos segundo y tercero del apartado 2 de este artículo.

4. El procedimiento podrá también tramitarse como consecuencia de la comunicación a la Agencia Española de Protección de Datos por parte de la autoridad de control de otro Estado miembro de la Unión Europea de la reclamación formulada ante la misma, cuando la Agencia Española de Protección de Datos tuviese la condición de autoridad de control principal para la tramitación de un procedimiento conforme a lo dispuesto en los artículos 56 y 60 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Será en este caso de aplicación lo dispuesto en los apartados 1, 2 y 3 de este artículo.

5. Los plazos de tramitación establecidos en este artículo así como los de admisión a trámite regulados por el artículo 65.5 y de duración de las actuaciones previas de investigación previstos en el artículo 67.2, quedarán automáticamente suspendidos cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de un órgano u organismo de la Unión Europea o de una o varias autoridades de control de los Estados miembros conforme con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Agencia Española de Protección de Datos.

6. El transcurso de los plazos de tramitación a los que se refiere el apartado anterior se podrá suspender, mediante resolución motivada, cuando resulte indispensable recabar información de un órgano jurisdiccional.

Se modifica por la disposición final 9.4 de la Ley 11/2023, de 8 de mayo. Ref. BOE-A-2023-11022#df-9

Artículo 65 Admisión a trámite de las reclamaciones.

1. Cuando se presentase ante la Agencia Española de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.

2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

3. Igualmente, la Agencia Española de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia Española de Protección de Datos, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado en el caso de las infracciones previstas en el artículo 74 de esta ley orgánica.

b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá remitir la misma al delegado de protección de datos que hubiera, en su caso, designado el responsable o encargado del tratamiento, al organismo de supervisión establecido para la aplicación de los códigos de conducta o al organismo que asuma las funciones de resolución extrajudicial de conflictos a los efectos previstos en los artículos 37 y 38.2 de esta ley orgánica.

La Agencia Española de Protección de Datos podrá igualmente remitir la reclamación al responsable o encargado del tratamiento cuando no se hubiera designado un delegado de protección de datos ni estuviera adherido a mecanismos de resolución extrajudicial de conflictos, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación en el plazo de un mes.

Si como consecuencia de dichas actuaciones de remisión, el responsable o encargado del tratamiento demuestra haber adoptado medidas para el cumplimiento de la normativa aplicable, la Agencia Española de Protección de Datos podrá inadmitir a trámite la reclamación.

5. La decisión sobre la admisión o inadmisión a trámite, así como la que determine, en su caso, la remisión de la reclamación a la autoridad de control principal que se estime competente, deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación con arreglo a lo dispuesto en este título a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia Española de Protección de Datos, sin perjuicio de la facultad de la Agencia de archivar posteriormente y de forma expresa la reclamación.

En el supuesto de que la Agencia Española de Protección de Datos actúe como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.4 de esta ley orgánica, el cómputo del plazo señalado en el párrafo anterior se iniciará una vez que se reciba en la Agencia toda la documentación necesaria para su tramitación.

Cuando los hechos de una reclamación relativa a la posible existencia en el ámbito competencial de la Agencia, guarden identidad sustancial con los que sean objeto de unas actuaciones previas de investigación o de un procedimiento sancionador ya iniciado, en la notificación de la decisión de admisión a trámite se podrá indicar el número de expediente correspondiente a las actuaciones previas o al procedimiento correspondiente, así como de la dirección web en la que se publicará la resolución que ponga fin al mismo, a efectos de que el reclamante pueda conocer el curso y resultado de la investigación.

6. Tras la admisión a trámite, si el responsable o encargado del tratamiento demuestran haber adoptado medidas para el cumplimiento de la normativa aplicable, la Agencia Española de Protección de Datos podrá resolver el archivo de la reclamación, cuando en el caso concreto concurran circunstancias que aconsejen la adopción de otras soluciones más moderadas o alternativas a la acción correctiva, siempre que no se hayan iniciado actuaciones previas de investigación o alguno de los procedimientos regulados en esta ley orgánica.

Se modifican los apartados 4 y 5 y se añade el 6 por la disposición final 9.5 de la Ley 11/2023, de 8 de mayo. Ref. BOE-A-2023-11022#df-9

Artículo 66 Determinación del alcance territorial.

1. Salvo en los supuestos a los que se refiere el artículo 64.4 de esta ley orgánica, la Agencia Española de Protección de Datos deberá, con carácter previo a la realización de cualquier otra actuación, incluida la admisión a trámite de una reclamación o el comienzo de actuaciones previas de investigación, examinar su competencia y determinar el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir.

2. Si la Agencia Española de Protección de Datos considera que no tiene la condición de autoridad de control principal para la tramitación del procedimiento remitirá, sin más trámite, la reclamación formulada a la autoridad de control principal que considere competente, a fin de que por la misma se le dé el curso oportuno. La Agencia Española de Protección de Datos notificará esta circunstancia a quien, en su caso, hubiera formulado la reclamación.

El acuerdo por el que se resuelva la remisión a la que se refiere el párrafo anterior implicará el archivo provisional del procedimiento, sin perjuicio de que por la Agencia Española de Protección de Datos se dicte, en caso de que así proceda, la resolución a la que se refiere el apartado 8 del artículo 60 del Reglamento (UE) 2016/679.

Se modifica el apartado 1 por la disposición final 9.6 de la Ley 11/2023, de 8 de mayo. Ref. BOE-A-2023-11022#df-9

Artículo 67 Actuaciones previas de investigación.

1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en la sección 2.ª del capítulo I del título VII de esta ley orgánica y no podrán tener una duración superior a dieciocho meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa.

Se modifica el apartado 2 por la disposición final 9.7 de la Ley 11/2023, de 8 de mayo. Ref. BOE-A-2023-11022#df-9

Artículo 68 Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora.

1. Concluidas, en su caso, las actuaciones a las que se refiere el artículo anterior, corresponderá a la Presidencia de la Agencia Española de Protección de Datos, cuando así proceda, dictar acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, en que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

2. Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679, el proyecto de acuerdo de inicio de procedimiento sancionador se someterá a lo dispuesto en el mismo.

Artículo 69 Medidas provisionales y de garantía de los derechos.

1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.

2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia Española de Protección de Datos una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.

TÍTULO IX

Régimen sancionador

Artículo 70 Sujetos responsables.

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

a) Los responsables de los tratamientos.

b) Los encargados de los tratamientos.

c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.

d) Las entidades de certificación.

e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título.

Artículo 71 Infracciones.

Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.

Artículo 72 Infracciones consideradas muy graves.

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.

b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.

c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento.

d) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica.

f) El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 10 de esta ley orgánica.

g) El tratamiento de datos personales relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 27 de esta ley orgánica.

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica.

i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica.

j) La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.

k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

l) La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679.

m) El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 32 de esta ley orgánica cuando la misma sea exigible.

ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

p) La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

2. Tendrán la misma consideración y también prescribirán a los tres años las infracciones a las que se refiere el artículo 83.6 del Reglamento (UE) 2016/679.

Artículo 73 Infracciones consideradas graves.

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del Reglamento (UE) 2016/679.

b) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del Reglamento (UE) 2016/679.

c) El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.

e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.

h) El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.

i) La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.

j) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del Reglamento (UE) 2016/679.

k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

l) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

m) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

n) No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679.

ñ) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del Reglamento (UE) 2016/679.

o) No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.

p) El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 28 de esta ley orgánica.

q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

s) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

u) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del Reglamento (UE) 2016/679 o cuando la ley establezca la obligación de llevar a cabo esa consulta.

v) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

w) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

x) La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado.

y) Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del Reglamento (UE) 2016/679.

z) El desempeño de funciones que el Reglamento (UE) 2016/679 reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 39 de esta ley orgánica.

aa) El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 42 y 43 de Reglamento (UE) 2016/679.

ab) El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.

ac) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 74 Infracciones consideradas leves.

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.

b) La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los

artículos 15 a 22 del Reglamento (UE) 2016/679, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.

c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de esta ley orgánica.

d) No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73 c) de esta ley orgánica.

e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del Reglamento (UE) 2016/679.

f) El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3 de esta ley orgánica.

h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE) 2016/679 o la inexactitud en la determinación de las mismas.

i) No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.

j) La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de este de las disposiciones del Reglamento (UE) 2016/679 o de esta ley orgánica, conforme a lo exigido por el artículo 28.3 del citado reglamento.

k) El incumplimiento por el encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al Reglamento (UE) 2016/679 y a la presente ley orgánica o en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

l) Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del Reglamento (UE) 2016/679.

m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de documentar cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica.

o) Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.

p) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

q) El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme a lo exigido por los apartados 1 y 5 del artículo 43 del Reglamento (UE) 2016/679.

r) El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 75 Interrupción de la prescripción de la infracción.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del acuerdo de inicio.

Se modifica el párrafo 2 por la disposición final 9.8 de la Ley 11/2023, de 8 de mayo. Ref. BOE-A-2023-11022#df-9

Artículo 76 Sanciones y medidas correctivas.

1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.

4. Será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción fuese superior a un millón de euros y el infractor sea una persona jurídica.

Cuando la autoridad competente para imponer la sanción sea una autoridad autonómica de protección de datos, se estará a su normativa de aplicación.

Artículo 77 Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.

f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público.

i) Las Universidades Públicas.

j) Los consorcios.

k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica.

Se modifica el apartado 2 por la disposición final 9.9 de la Ley 11/2023, de 8 de mayo. Ref. BOE-A-2023-11022#df-9

Artículo 78 Prescripción de las sanciones.

1. Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 y de esta ley orgánica prescriben en los siguientes plazos:

a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año.

b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.

c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

3. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

TÍTULO X

Garantía de los derechos digitales

Artículo 79 Los derechos en la Era digital.

Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.

Artículo 80 Derecho a la neutralidad de Internet.

Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

Artículo 81 Derecho de acceso universal a Internet.

1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.

2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.

3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.

4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.

5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.

6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

Artículo 82 Derecho a la seguridad digital.

Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.

Artículo 83 Derecho a la educación digital.

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las Administraciones educativas deberán incluir en el desarrollo del currículo la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

Se modifica el apartado 1 por la disposición final 4 de la Ley Orgánica 3/2020, de 29 de diciembre. Ref. BOE-A-2020-17264

Artículo 84 Protección de los menores en Internet.

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

Artículo 85 Derecho de rectificación en Internet.

1. Todos tienen derecho a la libertad de expresión en Internet.

2. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

Artículo 86 Derecho a la actualización de informaciones en medios de comunicación digitales.

Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.

Artículo 87 Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Artículo 88 Derecho a la desconexión digital en el ámbito laboral.

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Artículo 89 Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lu de trabajo.

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

Artículo 90 Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Artículo 91 Derechos digitales en la negociación colectiva.

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

Artículo 92 Protección de datos de los menores en Internet.

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

Artículo 93 Derecho al olvido en búsquedas de Internet.

1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Artículo 94 Derecho al olvido en servicios de redes sociales y servicios equivalentes.

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

Artículo 95 Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.

Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

Artículo 96 Derecho al testamento digital.

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

Artículo 97 Políticas de impulso de los derechos digitales.

1. El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público; y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

2. Asimismo se aprobará un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

3. El Gobierno presentará un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías y mandatos contemplados en el presente Título y de las medidas necesarias para promover su impulso y efectividad.

Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Disposición adicional segunda. Protección de datos y transparencia y acceso a la información pública.

La publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición adicional tercera. Cómputo de plazos.

Los plazos establecidos en el Reglamento (UE) 2016/679 o en esta ley orgánica, con independencia de que se refieran a relaciones entre particulares o con entidades del sector público, se regirán por las siguientes reglas:

a) Cuando los plazos se señalen por días, se entiende que estos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos.

b) Si el plazo se fija en semanas, concluirá el mismo día de la semana en que se produjo el hecho que determina su iniciación en la semana de vencimiento.

c) Si el plazo se fija en meses o años, concluirá el mismo día en que se produjo el hecho que determina su iniciación en el mes o el año de vencimiento. Si en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entenderá que el plazo expira el último día del mes.

d) Cuando el último día del plazo sea inhábil, se entenderá prorrogado al primer día hábil siguiente.

Disposición adicional cuarta. Procedimiento en relación con las competencias atribuidas a la Agencia Española de Protección de Datos por otras leyes.

Lo dispuesto en el Título VIII y en sus normas de desarrollo será de aplicación a los procedimientos que la Agencia Española de Protección de Datos hubiera de tramitar en ejercicio de las competencias que le fueran atribuidas por otras leyes.

Disposición adicional quinta. Autorización judicial en relación con decisiones de la Comisión Europea en materia de transferencia internacional de datos.

1. Cuando una autoridad de protección de datos considerase que una decisión de la Comisión Europea en materia de transferencia internacional de datos, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el Reglamento (UE) 2016/679, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente la suspensión del procedimiento, a fin de solicitar del órgano judicial autorización para declararlo así en el seno del procedimiento del que esté conociendo. Dicha suspensión deberá ser confirmada, modificada o levantada en el acuerdo de admisión o inadmisión a trámite de la solicitud de la autoridad de protección de datos dirigida al tribunal competente.

Las decisiones de la Comisión Europea a las que puede resultar de aplicación este cauce son:

a) aquellas que declaren el nivel adecuado de protección de un tercer país u organización internacional, en virtud del artículo 45 del Reglamento (UE) 2016/679;

b) aquellas por las que se aprueben cláusulas tipo de protección de datos para la realización de transferencias internacionales de datos, o

c) aquellas que declaren la validez de los códigos de conducta a tal efecto.

2. La autorización a la que se refiere esta disposición solamente podrá ser concedida si, previo planteamiento de cuestión prejudicial de validez en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea, la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

Disposición adicional sexta. Incorporación de deudas a sistemas de información crediticia.

No se incorporarán a los sistemas de información crediticia a los que se refiere el artículo 20.1 de esta ley orgánica deudas en que la cuantía del principal sea inferior a cincuenta euros.

El Gobierno, mediante real decreto, podrá actualizar esta cuantía.

Disposición adicional séptima. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

Disposición adicional octava. Potestad de verificación de las Administraciones Públicas.

Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

Disposición adicional novena. Tratamiento de datos personales en relación con la notificación de incidentes de seguridad.

Cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

Disposición adicional décima. Comunicaciones de datos por los sujetos enumerados en el artículo 77.1.

Los responsables enumerados en el artículo 77.1 de esta ley orgánica podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679.

Disposición adicional undécima. Privacidad en las comunicaciones electrónicas.

Lo dispuesto en la presente ley orgánica se entenderá sin perjuicio de la aplicación de las normas de Derecho interno y de la Unión Europea reguladoras de la privacidad en el sector de las comunicaciones electrónicas, sin imponer obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación en ámbitos en los que estén sujetas a obligaciones específicas establecidas en dichas normas.

Disposición adicional duodécima. Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.

1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.

2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.

3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

Disposición adicional decimotercera. Transferencias internacionales de datos tributarios.

Las transferencias de datos tributarios entre el Reino de España y otros Estados o entidades internacionales o supranacionales, se regularán por los términos y con los límites establecidos en la normativa sobre asistencia mutua entre los Estados de la Unión Europea, o en el marco de los convenios para evitar la doble imposición o de otros convenios internacionales, así como por las normas sobre la asistencia mutua establecidas en el Capítulo VI del Título III de la Ley 58/2003, de 17 de diciembre, General Tributaria.

Disposición adicional decimocuarta. Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE.

Las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.

Disposición adicional decimoquinta. Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores.

Cuando no haya podido obtener por otros medios la información necesaria para realizar sus labores de supervisión e inspección relacionadas con la detección de delitos graves, la Comisión Nacional del Mercado de Valores podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, los datos que obren en su poder relativos a la comunicación electrónica o servicio de la sociedad de la información proporcionados por dichos prestadores que sean distintos a su contenido y resulten imprescindibles para el ejercicio de dichas labores.

La cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales.

Se modifica por la disposición final 4.3 de la Ley Orgánica 7/2021, de 26 de mayo. Ref. BOE-A-2021-8806#df-4

Disposición adicional decimosexta. Prácticas agresivas en materia de protección de datos.

A los efectos previstos en el artículo 8 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, se consideran prácticas agresivas las siguientes:

a) Actuar con intención de suplantar la identidad de la Agencia Española de Protección de Datos o de una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos o a los interesados.

b) Generar la apariencia de que se está actuando en nombre, por cuenta o en colaboración con la Agencia Española de Protección de Datos o una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos en que la remitente ofrezca sus productos o servicios.

c) Realizar prácticas comerciales en las que se coarte el poder de decisión de los destinatarios mediante la referencia a la posible imposición de sanciones por incumplimiento de la normativa de protección de datos personales.

d) Ofrecer cualquier tipo de documento por el que se pretenda crear una apariencia de cumplimiento de las disposiciones de protección de datos de forma complementaria a la realización de acciones formativas sin haber llevado a cabo las actuaciones necesarias para verificar que dicho cumplimiento se produce efectivamente.

e) Asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos.

Disposición adicional decimoséptima. Tratamientos de datos de salud.

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del 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 sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:

1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.

2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.

3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Disposición adicional decimoctava. Criterios de seguridad.

La Agencia Española de Protección de Datos desarrollará, con la colaboración, cuando sea precisa, de todos los actores implicados, las herramientas, guías, directrices y orientaciones que resulten precisas para dotar a los profesionales, microempresas y pequeñas y medianas empresas de pautas adecuadas para el cumplimiento de las obligaciones de responsabilidad activa establecidas en el Título IV del Reglamento (UE) 2016/679 y en el Título V de esta ley orgánica.

Disposición adicional decimonovena. Derechos de los menores ante Internet.

En el plazo de un año desde la entrada en vigor de esta ley orgánica, el Gobierno remitirá al Congreso de los Diputados un proyecto de ley dirigido específicamente a garantizar los derechos de los menores ante el impacto de Internet, con el fin de garantizar su seguridad y luchar contra la discriminación y la violencia que sobre los mismos es ejercida mediante las nuevas tecnologías.

Disposición adicional vigésima. Especialidades del régimen jurídico de la Agencia Española de Protección de Datos.

1. No será de aplicación a la Agencia Española de Protección de Datos el artículo 50.2.c) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. La Agencia Española de Protección de Datos podrá adherirse a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes prevista en el artículo 85 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Disposición adicional vigésima primera. Educación digital.

Las Administraciones educativas darán cumplimiento al mandato contenido en el párrafo segundo del apartado 1 del artículo 83 de esta ley orgánica en el plazo de un año a contar desde la entrada en vigor de la misma.

Disposición adicional vigésima segunda. Acceso a los archivos públicos y eclesiásticos.

Las autoridades públicas competentes facilitarán el acceso a los archivos públicos y eclesiásticos en relación con los datos que se soliciten con ocasión de investigaciones policiales o judiciales de personas desaparecidas, debiendo atender las solicitudes con prontitud y diligencia las instituciones o congregaciones religiosas a las que se realicen las peticiones de acceso.

Disposición adicional vigésima tercera. Modelos de presentación de reclamaciones.

La Agencia Española de Protección de Datos podrá establecer modelos de presentación de reclamaciones ante la misma en todos los ámbitos en los que ésta tenga competencia, que serán de uso obligatorio para los interesados independientemente de que estén obligados o no a relacionarse electrónicamente con las administraciones públicas.

Los modelos serán publicados en el "Boletín Oficial del Estado" y en la Sede Electrónica de la Agencia Española de Protección de Datos y serán de obligado cumplimiento al mes de su publicación en el "Boletín Oficial del Estado".»

Se añade por la disposición final 9.10 de la Ley 11/2023, de 8 de mayo. Ref. BOE-A-2023-11022#df-9

Disposición transitoria primera. Estatuto de la Agencia Española de Protección de Datos.

1. El Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, continuará vigente en lo que no se oponga a lo establecido en el Título VIII de esta ley orgánica.

2. Lo dispuesto en los apartados 2, 3 y 5 del artículo 48 y en el artículo 49 de esta ley orgánica se aplicará una vez expire el mandato de quien ostente la condición de Director de la Agencia Española de Protección de Datos a la entrada en vigor de la misma.

Disposición transitoria segunda. Códigos tipo inscritos en las autoridades de protección de datos conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Los promotores de los códigos tipo inscritos en el registro de la Agencia Española de Protección de Datos o en las autoridades autonómicas de protección de datos deberán adaptar su contenido a lo dispuesto en el artículo 40 del Reglamento (UE) 2016/679 en el plazo de un año a contar desde la entrada en vigor de esta ley orgánica.

Si, transcurrido dicho plazo, no se hubiera solicitado la aprobación prevista en el artículo 38.4 de esta ley orgánica, se cancelará la inscripción y se comunicará a sus promotores.

Disposición transitoria tercera. Régimen transitorio de los procedimientos.

1. Los procedimientos ya iniciados a la entrada en vigor de esta ley orgánica se regirán por la normativa anterior, salvo que esta ley orgánica contenga disposiciones más favorables para el interesado.

2. Lo dispuesto en el apartado anterior será asimismo de aplicación a los procedimientos respecto de los cuales ya se hubieren iniciado las actuaciones previas a las que se refiere la Sección 2.ª del Capítulo III del Título IX del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Disposición transitoria cuarta. Tratamientos sometidos a la Directiva (UE) 2016/680.

Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.

Téngase en cuenta que la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, ha sido transpuesta por la Ley Orgánica 7/2021, de 26 de mayo. Ref. BOE-A-2021-8806

Disposición transitoria quinta. Contratos de encargado del tratamiento.

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

Disposición transitoria sexta. Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley orgánica.

Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:

a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento.

b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

Disposición derogatoria única. Derogación normativa.

1. Sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Queda derogado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

3. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición final primera. Naturaleza de la presente ley.

La presente ley tiene el carácter de ley orgánica.

No obstante, tienen carácter de ley ordinaria:

– El Título IV,

– el Título VII, salvo los artículos 52 y 53, que tienen carácter orgánico,

– el Título VIII,

– el Título IX,

– los artículos 79, 80, 81, 82, 88, 95, 96 y 97 del Título X,

– las disposiciones adicionales, salvo la disposición adicional segunda y la disposición adicional decimoséptima, que tienen carácter orgánico,

– las disposiciones transitorias,

– y las disposiciones finales, salvo las disposiciones finales primera, segunda, tercera, cuarta, octava, décima y decimosexta, que tienen carácter orgánico.

Disposición final segunda. Título competencial.

1. Esta ley orgánica se dicta al amparo del artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

2. El Capítulo I del Título VII, el Título VIII, la disposición adicional cuarta y la disposición transitoria primera sólo serán de aplicación a la Administración General del Estado y a sus organismos públicos.

3. Los artículos 87 a 90 se dictan al amparo de la competencia exclusiva que el artículo 149.1.7.ª y 18.ª de la Constitución reserva al Estado en materia de legislación laboral y bases del régimen estatutario de los funcionarios públicos respectivamente.

4. La disposición adicional quinta y las disposiciones finales séptima y sexta se dictan al amparo de la competencia que el artículo 149.1.6.ª de la Constitución atribuye al Estado en materia de legislación procesal.

5. La disposición adicional tercera se dicta al amparo del artículo 149.1.18.ª de la Constitución.

6. El artículo 96 se dicta al amparo del artículo 149.1.8.ª de la Constitución.

Disposición final tercera. Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

Se modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General que queda redactada como sigue:

Uno. El apartado 3 del artículo treinta y nueve queda redactado como sigue:

«3. Dentro del plazo anterior, cualquier persona podrá formular reclamación dirigida a la Delegación Provincial de la Oficina del Censo Electoral sobre sus datos censales, si bien solo podrán ser tenidas en cuenta las que se refieran a la rectificación de errores en los datos personales, a los cambios de domicilio dentro de una misma circunscripción o a la no inclusión del reclamante en ninguna Sección del Censo de la circunscripción pese a tener derecho a ello. También serán atendidas las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral. No serán tenidas en cuenta para la elección convocada las que reflejen un cambio de residencia de una circunscripción a otra, realizado con posterioridad a la fecha de cierre del censo para cada elección, debiendo ejercer su derecho en la sección correspondiente a su domicilio anterior.»

Dos. Se añade un nuevo artículo cincuenta y ocho bis, con el contenido siguiente:

«Artículo cincuenta y ocho bis. Utilización de medios tecnológicos y datos personales en las actividades electorales.

1. (Anulado)

2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»

Se declara contrario a la Constitución y nulo lo indicado del apartado 2 por Sentencia del TC 76/2019, de 22 de mayo. Ref. BOE-A-2019-9548

Disposición final cuarta. Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Se modifica la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, en los siguientes términos:

Uno. Se añade un apartado tercero al artículo 58, con la siguiente redacción:

«Artículo 58.

Tercero. De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por el Consejo General del Poder Judicial.»

Dos. Se añade una letra f) al artículo 66, con la siguiente redacción:

«Artículo 66.

f) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añaden una letra k) al apartado 1 y un nuevo apartado 7 al artículo 74, con la siguiente redacción:

«Artículo 74.

1. [...]

k) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.

[...]

7. Corresponde a las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia autorizar, mediante auto, el requerimiento de información por parte de autoridades autonómicas de protección de datos a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Cuatro. Se añade un nuevo apartado 7 al artículo 90:

«7. Corresponde a los Juzgados Centrales de lo Contencioso-administrativo autorizar, mediante auto, el requerimiento de información por parte de la Agencia Española de Protección de Datos y otras autoridades administrativas independientes de ámbito estatal a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Disposición final quinta. Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad.

Se añade un nuevo Capítulo II al Título VI de la Ley 14/1986, de 25 de abril, General de Sanidad con el siguiente contenido:

«CAPÍTULO II

Tratamiento de datos de la investigación en salud

Artículo 105 bis.

El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.»

Disposición final sexta. Modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

La Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, se modifica en los siguientes términos:

Uno. Se añade un nuevo apartado 7 al artículo 10:

«7. Conocerán de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.»

Dos. Se añade un nuevo apartado 5 al artículo 11:

«5. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añade un nuevo apartado 4 al artículo 12:

«4. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por el Consejo General del Poder Judicial.»

Cuatro. Se introduce un nuevo artículo 122 ter, con el siguiente tenor:

«Artículo 122 ter. Procedimiento de autorización judicial de conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos.

1. El procedimiento para obtener la autorización judicial a que se refiere la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, se iniciará con la solicitud de la autoridad de protección de datos dirigida al Tribunal competente para que se pronuncie acerca de la conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos con el Derecho de la Unión Europea. La solicitud irá acompañada de copia del expediente que se encontrase pendiente de resolución ante la autoridad de protección de datos.

2. Serán partes en el procedimiento, además de la autoridad de protección de datos, quienes lo fueran en el procedimiento tramitado ante ella y, en todo caso, la Comisión Europea.

3. El acuerdo de admisión o inadmisión a trámite del procedimiento confirmará, modificará o levantará la suspensión del procedimiento por posible vulneración de la normativa de protección de datos tramitado ante la autoridad de protección de datos, del que trae causa este procedimiento de autorización judicial.

4. Admitida a trámite la solicitud, el Tribunal competente lo notificará a la autoridad de protección de datos a fin de que dé traslado a quienes interviniesen en el procedimiento tramitado ante la misma para que se personen en el plazo de tres días. Igualmente, se dará traslado a la Comisión Europea a los mismos efectos.

5. Concluido el plazo mencionado en la letra anterior, se dará traslado de la solicitud de autorización a las partes personadas a fin de que en el plazo de diez días aleguen lo que estimen procedente, pudiendo solicitar en ese momento la práctica de las pruebas que estimen necesarias.

6. Transcurrido el período de prueba, si alguna de las partes lo hubiese solicitado y el órgano jurisdiccional lo estimase pertinente, se celebrará una vista. El Tribunal podrá decidir el alcance de las cuestiones sobre las que las partes deberán centrar sus alegaciones en dicha vista.

7. Finalizados los trámites mencionados en los tres apartados anteriores, el Tribunal competente adoptará en el plazo de diez días una de estas decisiones:

a) Si considerase que la decisión de la Comisión Europea es conforme al Derecho de la Unión Europea, dictará sentencia declarándolo así y denegando la autorización solicitada.

b) En caso de considerar que la decisión es contraria al Derecho de la Unión Europea, dictará auto de planteamiento de cuestión prejudicial de validez de la citada decisión ante el Tribunal de Justicia de la Unión Europea, en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea.

La autorización solamente podrá ser concedida si la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

8. El régimen de recursos será el previsto en esta ley.»

Disposición final séptima. Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Se modifica el artículo 15 bis de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que queda redactado como sigue:

«Artículo 15 bis. Intervención en procesos de defensa de la competencia y de protección de datos.

1. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas en el ámbito de sus competencias podrán intervenir en los procesos de defensa de la competencia y de protección de datos, sin tener la condición de parte, por propia iniciativa o a instancia del órgano judicial, mediante la aportación de información o presentación de observaciones escritas sobre cuestiones relativas a la aplicación de los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea o los artículos 1 y 2 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia. Con la venia del correspondiente órgano judicial, podrán presentar también observaciones verbales. A estos efectos, podrán solicitar al órgano jurisdiccional competente que les remita o haga remitir todos los documentos necesarios para realizar una valoración del asunto de que se trate.

La aportación de información no alcanzará a los datos o documentos obtenidos en el ámbito de las circunstancias de aplicación de la exención o reducción del importe de las multas previstas en los artículos 65 y 66 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

2. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas aportarán la información o presentarán las observaciones previstas en el número anterior diez días antes de la celebración del acto del juicio a que se refiere el artículo 433 o dentro del plazo de oposición o impugnación del recurso interpuesto.

3. Lo dispuesto en los anteriores apartados en materia de procedimiento será asimismo de aplicación cuando la Comisión Europea, la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, en el ámbito de sus competencias, consideren precisa su intervención en un proceso que afecte a cuestiones relativas a la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.»

Disposición final octava. Modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

Se incluye una nueva letra l) en el apartado 2 del artículo 46 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, con el contenido siguiente:

«l) La formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.»

Disposición final novena. Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Se modifica el apartado 3 del artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que pasa a tener el siguiente tenor:

«Artículo 16. [...]

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.»

Disposición final décima. Modificación de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

Se incluye una nueva letra l) en el apartado 1 del artículo 2 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, que queda redactado como sigue:

«l) La capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva.»

Disposición final undécima. Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Se modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en los siguientes términos:

Uno. Se añade un nuevo artículo 6 bis, con la siguiente redacción:

«Artículo 6 bis. Registro de actividades de tratamiento.

Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.»

Dos. El apartado 1 del artículo 15 queda redactado como sigue:

«1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del

afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.»

Disposición final duodécima. Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Se modifican los apartados 2 y 3 del artículo 28 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que pasan a tener la siguiente redacción:

«Artículo 28. [...]

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.»

Disposición final decimotercera. Modificación del texto refundido de la Ley del Estatuto de los Trabajadores.

Se añade un nuevo artículo 20 bis al texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, con el siguiente contenido:

«Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.

Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimocuarta. Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.

Se añade una nueva letra j bis) en el artículo 14 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, que quedará redactada como sigue:

«j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimoquinta. Desarrollo normativo.

Se habilita al Gobierno para desarrollar lo dispuesto en los artículos 3.2, 38.6, 45.2, 63.3, 96.3 y disposición adicional sexta, en los términos establecidos en ellos.

Disposición final decimosexta. Entrada en vigor.

La presente ley orgánica entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

Por tanto,

Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta ley orgánica.

Madrid, 5 de diciembre de 2018.

FELIPE R.

El Presidente del Gobierno,

PEDRO SÁNCHEZ PÉREZ-CASTEJÓN