7. Protección de datos de carácter personal

Vicenta Colás Gil

Secretaria-Interventora del Servicio Cuarto Espacio de la Diputación Provincial de Zaragoza

SUMARIO

1. Introducción.

2. Normativa.

3. La Protección de datos de carácter personal en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y en el Real Decreto 1720/2007, de 21 de diciembre.

4. La Agencia Española de Protección de Datos.

5. El nuevo Reglamento General de Protección de Datos.

6. El Proyecto de Ley Orgánica de Protección de Datos Personales y Garantías de los Derechos Digitales.

7. La Videovigilancia.

8. 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.

9. Preguntas habituales sobre protección de datos.

1. INTRODUCCIÓN

En nuestra sociedad, las nuevas tecnologías de la información y la comunicación nos permiten estar conectados en todo momento, pero también abren la puerta a nuevas amenazas e injerencias en nuestra privacidad.

Esta irrupción de las nuevas tecnologías esta provocando que los ciudadanos veamos con frecuencia que algunos de nuestros derechos fundamentales se ven lesionados por personas que utilizan dichas tecnologías en su propio beneficio, aprovechando el desconocimiento de las mismas por parte de los interesados.

Los aspectos que se están viendo más afectados por este avance tecnológico es la utilización por parte de empresas y Administraciones Públicas de los datos personales de sus usuarios, como herramienta para descubrir sus perfiles, conocer sus ideas… etc., en definitiva, controlar en cierta forma nuestras actividades cotidianas.

El Legislador y los Tribunales, que velan por la protección de los derechos fundamentales de las personas físicas, tanto en el ámbito europeo, como en el español, frente a esta amenaza, se han esforzado para que dicha protección sea efectiva, para la cual se ha considerado que el derecho a la protección de datos de carácter personal *«es un nuevo derecho fundamental»*.

El derecho fundamental a la protección de datos de carácter personal es el resultado de una paulatina construcción constitucional, legislativa y, sobre todo, jurisprudencial.

Hoy liberado ya de su congénita servidumbre respecto de la protección de la intimidad, el derecho a la protección de datos de carácter personal se configura por fin como un derecho fundamental autónomo. Constituye el derecho fundamental característico de esa faceta del mundo social que comúnmente llamamos Sociedad de la Información, en la que opera como *«un elemento constitutivo de la libertad del ciudadano»*.

La protección de datos puede ser considerada *«el nuevo derecho fundamental del siglo XXI»*.

La consagración de este derecho después de que se promulga la Constitución Española, se produce con la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

Hasta llegar a considerar la protección de datos como un derecho fundamental e independiente, no ha sido fácil, los primeros problemas suscitados en el tema se solucionaban con el «derecho a la intimidad», hasta que se forjo el derecho actual.

El derecho fundamental a la protección de datos de carácter personal, persigue garantizar a la persona nacional o extranjera el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para su dignidad y sus derechos, así como para oponerse a cualquier reconstrucción, conocida o no, de su identidad, su comportamiento o su ideología y su opinión a partir de sus datos personales por quien los posea.

Ha sido el Tribunal Constitucional quien ha considerado que en el apartado 4 del artículo 18[110] de la Constitución Española se garantiza un nuevo derecho fundamental *«El derecho fundamental a la protección de datos de carácter personal»* (STC 292/2000).

El derecho a la protección de datos consiste en un poder sobre el uso del dato revelado, poniendo a disposición del afectado la facultad de controlar ese uso y el destino del dato que revela a un tercero con el fin de atajar el uso fraudulento o el tráfico ilegal de sus datos personales, e incluso cualquier evaluación de su persona que se haga a partir de ellos, si la obtención, el almacenamiento y el tratamiento de esos datos se ha hecho sin su conocimiento y consentimiento.

El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos, e impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o la divulgación indebidos de dicha información.

110 Art. 18.4 CE «La Ley limitará el uso de la informática para garantizar el honor v la intimidad personal v familiar de los ciudadanos v el pleno ejercicio de sus derechos».

La Agencia Española de Protección de Datos, describe el derecho a la Protección de datos en su Guía del Derecho Fundamental a la Protección de Datos de Carácter Personal como: «*El derecho fundamental a la protección de datos reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos*».

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

La nueva reforma de la legislación sobre protección de datos pretende garantizar que los ciudadanos tengan el control de su información personal en el mundo digital.

El objeto de este derecho fundamental es la protección de los datos de carácter personal.

Por este motivo nos preguntamos: ¿qué es un dato de carácter personal?

—Es la información relativa a una persona que permita su identificación.

—En palabras de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de *Datos de Carácter Personal: «Cualquier información concerniente a personas físicas identificadas o identificables» (artículo 3.a)*.

—En un sentido más amplio: «Toda información numérica, alfabética, gráfica, *fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables»* (artículo 5 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).

—Definición que da el Reglamento General de Protección de Datos: Datos personales: Toda información sobre una persona física identificada o identificable («el interesado»). Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.[111]

2. NORMATIVA

En el ámbito de las Administraciones Públicas, que manejan cantidades ingentes de datos personales, la transmisión de los mismos entre dichas Administraciones podría dar lugar a la creación de *una gran base de datos que permitiera conocer con gran exactitud los perfiles de los ciudadanos*, lo que supondría una grave carencia de libertad de los mismos.

De ahí la importancia que las Administraciones Públicas sean muy escrupulosas en el respeto a la normativa existente en materia de protección de datos de carácter personal.

La legislación de protección de datos de carácter personal surgió como medida para frenar el imparable uso y abuso que se hace de los datos de carácter personal de las personas físicas y que se ha potenciado, aun más, a través del uso de las nuevas tecnologías, como el INTERNET. Se puede consultar en la página web de la Agencia Española de Protección de Datos (*http://www.agpd.es*):

1. Normativa europea, estatal y autonómica.

2. Instrucciones de la Agencia Española de Protección de Datos (AEPD).

3. Resoluciones de la AEPD.

4. Recomendaciones de la AEPD.

5. Sentencias del Tribunal Constitucional, Tribunal Supremo, Tribunales Superiores de Justicia, Tribunal de Justicia de la Comunidades Europeas, de la Audiencia Nacional.

Vamos a destacar:

—La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). A partir del 25 de mayo de 2018, es aplicable el RGPD, este desplaza los preceptos de esta Ley que no resulten conformes con el régimen que el mismo establece.

—El Real Decreto 1720/2007, de 21 de diciembre, por el que sea aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RLOPD). A partir del 25 de mayo de 2018, es aplicable el RGPD, este desplaza los preceptos de este Real Decreto, que no resulten conformes con el régimen que el mismo establece.

—El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).

• El RGPD se aprobó en el mes de abril de 2016 y entró en vigor el 25 de mayo de 2016. Es aplicable desde el 25 de mayo de 2018.

• El Reglamento General de Protección de Datos (RGPD):

–Se encuadra en la reforma normativa realizada por la Unión Europea con el objetivo de garantizar unos estándares de protección de datos elevados y adaptados a la realidad digital del mundo actual.

–Moderniza la normativa europea sobre protección de datos y unifica las legislaciones de los Estados miembros.

–Es una norma directamente aplicable a todos los Estados miembros.

–Modifica algunos aspectos del régimen actual y contiene nuevas obligaciones.

—El Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, que 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.

—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.

111 El RGPD es aplicable desde el 25 de mayo de 2018

3. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y EN EL REAL DECRETO 1720/2007, DE 21 DE DICIEMBRE

La normativa a la que nos vamos a referir en este apartado de una manera breve es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RLOPD).

Es importante tener en cuenta que desde el 25 de mayo de 2018, se aplica el nuevo Reglamento General de Protección de Datos.

La plena aplicación del RGPD implica que hayan de considerarse desplazadas por el aquellas disposiciones de Derecho interno que no resulten conformes con el régimen que el mismo establece. Así sucederá con muchos de los preceptos de la LOPD y el RLOPD.

El RGPD supone una profunda modificación del régimen vigente en materia de protección de datos, no solo desde el punto de vista sustantivo y de cumplimiento por los sujetos obligados, sino particularmente en lo que afecta a la actividad de supervisón por parte de las autoridades de control que el mismo regula.

3.1. La LOPD. Objeto y Ámbito de aplicación

La Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), adaptó nuestro ordenamiento a lo dispuesto por 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, derogando a su vez a la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal (LORTAD).

3.1.1. Objeto de la LOPD

Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Además comprende el tratamiento automatizado y el no automatizado de los datos de carácter personal.

3.1.2. Ámbito de aplicación

3.1.2.1.Ámbito objetivo.

La LOPD es aplicable a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

—Están excluidos de la LOPD:

• Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

• Los ficheros sometidos a la normativa sobre protección de materias clasificadas.

• Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

—Se regirán por sus disposiciones específicas:

• Los ficheros regulados por la legislación de régimen electoral.

• Ficheros exclusivamente estadísticos.

• Fuerzas armadas.

• Registro Civil y Registro de penados y rebeldes.

• Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las fuerzas y Cuerpos de seguridad.

3.1.2.2.Ámbito espacial.

—Se regirá por la LOPD todo tratamiento de datos de carácter personal:

• Cuando el tratamiento sea efectuado en territorio español en el marco de la actividad de un establecimiento del responsable del tratamiento.

• Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional Público.

• Cuando el responsable de tratamiento no esté establecido en territorio de la Unión Europea y utilice el tratamiento de los datos medios situados en territorio español, salvo que se utilicen únicamente con fines de tránsito.

3.1.2.3. Ámbito subjetivo.

La LOPD trata de proteger los derechos fundamentales y las libertades públicas y en particular el derecho a la intimidad y el honor de las personas físicas.

3.2. El Real Decreto 1720/ 2007, de 21 de diciembre, por el que sea aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Viene a abarcar el ámbito tutelado anteriormente por los Reales Decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados.

Este Reglamento comparte con la LOPD la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales.

Tiene por objeto el desarrollo de la LOPD.

Una de las novedades es la aplicación de las medidas de seguridad a los ficheros en papel.

3.3. Los Principios de la protección de datos de carácter personal

En la LOPD se enumeran los principios de la protección de datos de carácter personal en el título II. De estos principios se derivan una serie de derechos para las personas afectadas.

—Los principios de la protección de datos son los siguientes:

3.3.1. Calidad de los datos

Los datos recogidos serán adecuados, pertinentes y no excesivos atendiendo a la finalidad para la que han sido recabados.

Los datos de carácter personal:

—No podrán usarse para finalidades incompatibles para las que fueron recogidas.

—Serán exactos y puestos al día.

—Serán cancelados cuando dejen de ser necesarios y cuando no sean exactos o estén incompletos.

—No se podrán recoger los datos por medios fraudulentos, desleales o ilícitos, salvo que se mantengan para valores históricos, científicos o estadísticos, una vez que dejen de ser útiles para la función requerida no podrán ser conservados.

—Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

El RLOPD, introduce algunas novedades importantes en relación con este principio:

—La consideración de datos exactos, si son obtenidos del interesado.

—La posibilidad de cancelar o sustituir datos inexactos o incompletos en un plazo de diez días, desde que se tenga constancia del hecho.

—La obligación de comunicar en el mismo plazo (10 días) los datos que han sido objeto de cesión, para proceder a su rectificación o cancelación.

—Introduce el término «bloqueo» de los datos para un fin concreto y un tiempo determinado (en caso de responsabilidades jurídicas o contractuales) tras el cual deberán suprimirse.

3.3.2. Derecho a la información en la recogida de datos

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

—De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.

—Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

—De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

—De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

—De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Este deber de información deberá llevarse a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

Cuando se utilicen cuestionarios o impresos para la recogida de datos, se harán constar estas advertencias.

La normativa diferencia entre dos situaciones: que los datos se recojan directamente del interesado o no. En el primero de los casos, el deber de información deberá realizarse con carácter previo a la recogida de los datos personales. Si los datos de carácter personal no han sido recabados del interesado deberá ser informado por el responsable del fichero, en el plazo de tres meses a contar desde el momento del registro de los datos, del contenido del tratamiento, de la procedencia de los datos, de la existencia del fichero, su finalidad, de la posibilidad de ejercitar los derechos, de la identidad y dirección del responsable.

Por último hemos de mencionar una excepción de conformidad con lo señalado en el artículo 24 de la LOPD: «Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales».

3.3.3. Consentimiento del afectado

El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado.

No será necesario en los siguientes casos:

—Cuando se recojan para el ejercicio de funciones propias de la Administración Pública en el ámbito de sus competencias.

—Cuando sean necesarios para la realización de un contrato o precontacto.

—Cuando tenga por finalidad proteger un interés vital del interesado.

—Cuando se recojan de fuentes accesibles al público.

El consentimiento podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y en tanto que una Ley no disponga lo contrario, el afectado podrá oponerse al tratamiento, siempre que existan motivos fundados y legítimos relativos a una determinada situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

La forma en que el interesado debe manifestar o no su consentimiento, para que sea aceptado legalmente, debe cumplir los siguientes requisitos:

—Libre.

—Específico.

—Informado.

—Inequívoco.

Los tipos de consentimiento que reconoce la LOPD, son:

—Tácito. Cuando el titular de los datos personales no hace ninguna manifestación, ni a favor ni en contra. Se acepta este tipo de consentimiento salvo en los supuestos en los que se exige una declaración o manifestación expresa del consentimiento.

—Expreso. Cuando si existe del titular de los datos de carácter personal la manifestación que acepta el tratamiento de sus datos. Pude darse por escrito, verbalmente, mediante comunicación telemática o por cualquier otro medio.

El RLOPD, en su artículo 14 regula la forma de recabar el consentimiento. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo que la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

El responsable debe dirigirse al interesado o afectado informándole del tratamiento de los datos y de su finalidad, así como de las condiciones en las que se va a realizar. El afectado dispone de un plazo de 30 días para manifestar su negativa al tratamiento. Se le advierte que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

El responsable del fichero tiene la obligación de facilitar al interesado un medio sencillo y gratuito para manifestar su negativa a tratamiento de datos. Ejemplos: envío prefranqueado, servicios de atención al público puestos a disposición para tal fin, llamada un número de teléfono gratuito.

Así mismo en el apartado 5 del artículo 14 del RLOPD, señala: «Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud».

El RLOPD en su artículo 15, hace referencia a la solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma, en estos caso el responsable del tratamiento está obligado a habilitar una casilla para que el afectado exprese de forma explícita su negativa al tratamiento o comunicación de datos ajenos a la naturaleza del contrato.

EL artículo 17 del RLOPD recoge los medios y actuaciones mediante los cuales el titular de los datos puede revocar su consentimiento y en que plazos.

3.3.4. Consentimiento para el tratamiento de menores de edad

Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

3.3.5. Datos especialmente protegidos

Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias.

Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual solo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas solo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Podrán ser objeto de tratamiento los datos de carácter personal referidos (especialmente protegidos) cuando resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto y cuando sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

3.3.6. Datos relativos a la salud

Sin perjuicio de lo dispuesto en el artículo de la 11 LOPD sobre la cesión, las instituciones, centros sanitarios, y los profesionales podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Para la cesión de datos es preciso el consentimiento del afectado salvo los supuestos previstos en el artículo 11.2 f) de la LOPD (solucionar urgencias o estudios epidemiológicos).

3.3.7. Seguridad de los datos

El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a la integridad y seguridad y a los centros de tratamiento, locales, equipos, sistemas y programas.

3.3.8. Deber de secreto

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

3.3.9. Comunicación de datos

Por comunicación o cesión de datos se entiende toda aquella información que se revela a un tercero distinto del afectado.

Los datos de carácter personal objeto del tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

No será preciso:

—Cuando se autorice en una Ley.

—Cuando se trate de datos recogidos de fuentes accesibles al público.

—Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica.

—Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, etc.

—Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

—Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Será nulo el consentimiento, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

Aquel a quien se comuniquen los datos de carácter personal se obliga a la observancia de las disposiciones de la Ley.

Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

3.3.10. Acceso a los datos por cuenta de terceros

No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Estos principios referidos, han sido objeto de modificación por el nuevo Reglamento General de Protección de Datos, el cual es de plena aplicación desde el 25 de mayo de 2018. Además añade nuevos principios. Todo ello será objeto de posterior estudio en el apartado correspondiente del RGPD.

3.4. Los Derechos de las personas[112]

En función de los principios que hemos visto enumerados con anterioridad emergen una serie de derechos para las personas. Estos pueden colisionar con otros derechos igualmente legítimos.

Nuestro ordenamiento jurídico prevé los cauces necesarios para la tutela de todos los derechos, y asimismo articula los mecanismos para la ponderación de los mismos en caso de colisión entre ellos.

Vamos a señalar los derechos de las personas en relación con el derecho fundamental a la protección de datos de carácter personal que se recogen en la LOPD:

3.4.1. Impugnación de valoraciones

Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

3.4.2. Derecho de consulta al Registro General de Protección de Datos

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

El Registro General será de consulta pública y gratuita.

3.4.3. Derecho de información

El derecho de información, previo al tratamiento de los datos de carácter personal, es uno de los derechos básicos y principales contenidos en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

Si se van a registrar y tratar datos de carácter personal, será necesario informar previamente a los interesados, a través del medio que se utilice para la recogida, de modo expreso, preciso e inequívoco:

—De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.

—Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

—De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

—De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

—De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las referidas advertencias.

3.4.4. Derecho de acceso

El derecho de acceso reconoce al ciudadano el que pueda controlar por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a obtener información sobre si estos están siendo objeto de tratamiento y, en su caso, la finalidad del mismo, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

Su ejercicio es personalísimo, por lo que solo podrá solicitarlo la persona interesada, quién deberá dirigirse a la empresa u organismo público del que sabe o presume que tiene sus datos, pudiendo optar por visualizarlos directamente en pantalla u obtenerlos por medio de escrito, copia, fotocopia o cualquier otro sistema adecuado al tipo de fichero de que se trate.

El responsable del fichero deberá resolver sobre lo solicitado en el plazo de un mes desde la recepción de la solicitud. También deberá hacerlo aunque no disponga de datos del afectado. Si transcurrido dicho plazo, la solicitud no ha sido atendida adecuadamente, el interesado podrá dirigirse a la Agencia Española de Protección de datos(AEPD) con copia de la solicitud cursada y de la contestación recibida (si existiera), para que esta a su vez se dirija a la oficina designada con el objetivo de hacer efectivo el ejercicio de ese derecho.

El derecho de acceso no puede ser ejercitado en intervalos inferiores a 12 meses, salvo que se acredite un interés legitimo.

El interesado solo podrá acceder a la información pretendida si se trata de información sobre sus datos personales, pero no de información de terceros. Antes de dirigirse a la Agencia, deberá hacerlo ante la empresa u organismo responsable/titular del fichero donde estén sus datos.

112 En la página web de la AEPD. Se facilita modelos para el ejercicio de los derechos de las personas:- Ejercicio ante el responsable del fichero. - Solicitud de tutela ante la AGPD. - Instrucciones para la cumplimentación de los formularios.

3.4.5. Derecho de rectificación

El derecho de rectificación reconoce al ciudadano el que pueda defender su privacidad controlando por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a que estos se modifiquen cuando resulten inexactos o incompletos.

Su ejercicio es personalísimo, por lo que solo podrá solicitarlo la persona interesada, quién deberá dirigirse a la empresa u organismo público que sabe o presume que tiene sus datos, indicando a qué datos se refiere y la corrección que se solicita, y aportando al efecto la documentación que lo justifique.

El responsable del fichero deberá resolver sobre lo solicitado en el plazo máximo de diez días a contar desde la recepción de la solicitud. También deberá hacerlo aunque no disponga de datos del afectado. Transcurrido el plazo sin que de forma expresa se responda a la petición o esta sea insatisfactoria, el interesado podrá interponer la correspondiente reclamación de tutela ante la Agencia Española de Protección de Datos, acompañando la documentación acreditativa de haber solicitado la rectificación de datos ante la entidad de que se trate.

Antes de dirigirse a la Agencia, deberá hacerlo ante la empresa u organismo responsable/titular del fichero donde estén sus datos.

3.4.6. Derecho de cancelación

El derecho de cancelación reconoce al ciudadano el que pueda defender su privacidad controlando por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a que estos se supriman cuando resulten inadecuados o excesivos.

Su ejercicio es personalísimo, por lo que solo podrá solicitarlo la persona interesada, quién deberá dirigirse a la empresa u organismo público que sabe o presume que tiene sus datos, indicando a qué datos se refiere, y aportando al efecto a documentación que lo justifique.

El responsable del fichero deberá resolver sobre la solicitud de cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Deberá hacerlo aunque no disponga de datos del afectado. Transcurrido el plazo sin que de forma expresa se responda a la petición o esta sea insatisfactoria, el interesado podrá interponer la correspondiente reclamación de tutela ante la Agencia, acompañando la documentación acreditativa de haber solicitado la cancelación ante la entidad de que se trate.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de estas, transcurrido el cual deberá procederse a la cancelación.

No procederá la cancelación cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las relaciones contractuales entre la entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos, y también que, antes de dirigirse a la AEPD, deberá hacerlo ante la empresa o organismo responsable/titular del fichero donde estén sus datos.

Procedimientos de oposición, acceso, rectificación o cancelación.

Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

3.4.7. Tutela de los derechos

Las actuaciones contrarias a la LOPD pueden ser objeto de reclamación por los interesados ante la Agencia Española de Protección de Datos, en la forma que reglamentariamente se determine.

El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la AEPD o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

Contra las resoluciones de la Agencia Española de Protección de Datos procederá recurso contencioso-administrativo.

3.4.8. Derecho a indemnización

Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la LOPD por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

Estos derechos referidos, han sido objeto de modificación por el nuevo Reglamento General de Protección de Datos, el cual es de plena aplicación desde el 25 de mayo de 2018. Además añade nuevos derechos. Todo ello será objeto de posterior estudio en el apartado correspondiente del RGPD.

3.5. Obligaciones legales de las Administraciones Locales en materia de protección de datos de carácter personal

Las obligaciones legales de las Administraciones Locales en materia de protección de datos de carácter personal, son las siguientes:

—Creación, modificación o supresión de los ficheros del Ayuntamiento por medio de disposición general o acuerdo publicado en el B.O.P.

—Notificación a la AEPD de los ficheros de datos de carácter personal para su inscripción en Registro General de la AEPD en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el BOP. Se presentarán a través de medios telemáticos o en soporte papel.

—Redacción del documento de seguridad.

—Realizar un tratamiento legal de los datos cumpliendo todos los principios de actuación previstos en la LOPD referentes a la calidad de los datos, la información debida al titular de los datos, el consentimiento de este como regla general para el tratamiento, la existencia de datos que requieren una especial protección, la seguridad de los datos y las relaciones con terceros en las que se proceda a la cesión o comunicación de datos o al acceso a los datos por cuenta de terceros.

—Redacción de contratos, formularios y cláusulas necesarias para la recogida de datos y solicitud de consentimiento para la recogida y tratamiento de datos especialmente protegidos.

Estas obligaciones referidas, han sido objeto de modificación por el nuevo Reglamento General de Protección de Datos, el cual es de plena aplicación desde el 25 de mayo de 2018. Todo ello será objeto de posterior estudio en el apartado correspondiente del RGPD.

3.6. Ficheros y niveles de seguridad

La LOPD, a través de su Reglamento de desarrollo, obliga a las Administraciones Públicas, que almacenen, traten y accedan a ficheros de datos de carácter personal, a aplicar una serie de medidas de seguridad de carácter técnico y organizativo que garanticen la confidencialidad, integridad y disponibilidad de la información.

Las medidas deberán ser adoptadas e implantadas por el responsable del fichero, y en su caso por el Encargado del Tratamiento donde se traten datos de carácter personal. Las medidas se pueden clasificar de la siguiente forma:

—Medidas organizativas, destinadas a establecer procedimientos, normas, reglas y estándares de aplicación, que garanticen la seguridad y cuyos destinatarios son los usuarios que tratan los datos de los ficheros.

—Medidas técnicas, destinadas principalmente a conservar la integridad física e la información, para evitar robos, pérdidas o alteraciones no justificadas.

Estas medidas serán de aplicación a todos aquellos ficheros que contengan datos de carácter personal, independientemente de su soporte (electrónico o papel), así como a los locales donde se almacenan dichos datos y los continentes que los soportan (armarios, archivadores, ordenadores, servidores, etc.).

A los ficheros de datos de carácter personal se les aplica las medidas de seguridad según el grado de información sensible que contienen, en relación con la mayor o menor necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información.

El RD 1720/2007, establece la obligación de aplicar diferentes medidas de seguridad en función del nivel básico, medio o alto de los datos tratados.

Con la aplicación del RGPD, las medidas de seguridad ya no se aplican en función del nivel básico, medio o alto de los datos tratados. El RGPD condiciona la adopción de las medidas de seguridad a efectuar un análisis de riesgos. Sobre los resultados de ese análisis, se implantarán las medidas técnicas y organizativas necesarias para hacer frente a los riesgos detectados sobre los derechos y libertades de los ciudadanos.

3.7. Infracciones y Sanciones

Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la LOPD.

Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46 y 48 de la LOPD (el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas).

Las infracciones se calificaran como leves, graves y muy graves, se regulan en la LOPD. Los tipos de sanciones irán en función del tipo de infracción.

Con la aplicación del nuevo RGPD desde el 25 de mayo de 2018 este apartado se modifica, lo veremos en el apartado correspondiente del RGPD.

Además 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, con referencia al Régimen Sancionador en materia de protección de datos, articula el novedoso régimen sancionador establecido en el Reglamento General de Protección de Datos, reemplazando los tipos infractores actualmente contenidos en la Ley Orgánica 15/1999, por la remisión a los que están establecidos en los apartados 4, 5 y 6 del artículo 83 de dicho Reglamento, lo que resulta de todo punto necesario.

Este Real Decreto, deroga en concreto los artículos de la LOPD:

a) El artículo 40 «Potestad de inspección».

b) Los artículos 43 al 49, con excepción del artículo 46.[113]

4. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)

La defensa de los derechos de los afectados, así como la garantía de que la Ley se va a aplicar correctamente, exige la existencia de un organismo independiente que vele porque esto ocurra así.

La LOPD, ha optado por una solución un tanto atípica que constituye una variante de la opción de autoridad administrativa independiente y a la vez de la del Comisario o Defensor de los datos.

Se ha creado un Ente público independiente (la Agencia Española de protección de Datos) que según el artículo 35 de la LOPD «se *regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno»*.

La Agencia Española de Protección de Datos (AEPD) es la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos y garantiza y tutela el derecho fundamental a la protección de datos personales.

INFORMA y AYUDA al ciudadano a ejercitar sus derechos y a las entidades públicas y privadas a cumplir las obligaciones que establece la Ley.

TUTELA al ciudadano en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido adecuadamente atendidos.

Y GARANTIZA el derecho a la protección de datos investigando y sancionado aquellas actuaciones que puedan ser contraria a la Ley.

En el nuevo Reglamento General de Protección de Datos, que es de aplicación directa desde el 25 de mayo de 2018, su artículo 51 con referencia a la «Autoridad de Control», dispone:

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

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

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

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

El proyecto de Ley Orgánica de Protección de Datos que se está tramitando establece que la Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en el artículo 109 de la Ley 40/2015 como integrante del sector público institucional estatal, con plena personalidad jurídica y plena capacidad pública y privada que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones, y que se relaciona con el Gobierno a través del Ministerio de Justicia.

113 Titulo VII de la LOPD. Infracciones y Sanciones : artículo 43 de la LOPD « Responsables», artículo 44 de la LOPD « Tipos de infracciones», artículo 45 de la LOPD «Tipo de sanciones», artículo 46 de la LOPD «Infracciones de las Administraciones Públicas», artículo 47 de la LOPD « Prescripción», artículo 48 de la LOPD «Procedimiento sancionador», y artículo 49 de la LOPD « Potestad de inmovilización de ficheros».

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, hace referencia entre otros aparatados al *«Ámbito y personal competente para el ejercicio de la actividad de investigación de la Agencia Española de Protección de Datos»,* lo veremos con más detalle en el apartado correspondiente.

5. EL NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

El Reglamento General de Protección de Datos, se encuadra en la reforma normativa realizada por la Unión Europea con el objetivo de garantizar unos estándares de protección de datos elevados y adaptados a la realidad digital del mundo actual.

Su ámbito de aplicación se extiende a todos los países miembros de la Unión Europea y se aplica directamente en todos ellos desde 25 de mayo de 2018, fecha en la que todos los responsables y encargados de tratamiento habrán de haberse adecuado a sus previsiones.

5.1. La adaptación al RGPD

Las actuaciones que deben emprender los responsables y los encargados del tratamiento, para adecuar su actividad a la nueva regulación, son:[114]

—Designar un Delegado de Protección de Datos, si procede (artículo 34 del RGPD).

—Elaborar el Registro de actividades de tratamiento, prestando atención especialmente a los tratamientos que incluyan categorías especiales de datos o datos de menores, teniendo en cuenta su finalidad y la base jurídica.

—Analizar las bases jurídicas de los tratamientos.

—Efectuar un análisis de riesgos. Sobre los resultados de ese análisis, identificar e implantar las medidas técnicas y organizativas necesarias para hacer frente a los riesgos detectados sobre los derechos y libertades de los ciudadanos.

—Verificar las medidas de seguridad tras el resultado del análisis de riesgos. Ello incluye verificar la aplicación de medidas de seguridad adecuadas, así como establecer protocolos para gestionar y, en su caso, notificar quiebras de seguridad.

—Si el tratamiento es de alto riesgo, detallar e implantar un procedimiento para realizar, una evaluación de impacto de la privacidad y, si fuera necesario, consultar previamente a la autoridad de control (artículos 35 y 36 del RGPD).

En paralelo:

—Adecuar los formularios para adaptar el derecho de información a los requisitos del RGPD.

—Adaptar los procedimientos para atender los derechos de los ciudadanos, habilitando medios electrónicos.

—Establecer y revisar los procedimientos para acreditar el consentimiento y garantizar la posibilidad de revocarlo.

—Valorar si los encargados de tratamiento ofrecen garantías de cumplimiento del RGPD y adaptar los contratos elaborados previamente.

—Confeccionar e implantar políticas de protección de datos que contemplen los requisitos del RGPD (artículos 24, 25 y 30)[115] y poder acreditar su cumplimiento.

—Elaborar y llevar a cabo un plan de formación y concienciación para los empleados.

5.2. Principales novedades del RGPD

El RGPD**,** entró en vigor el 25 de mayo de 2016 y es de aplicación directa desde el 25 de mayo de 2018.

Deroga: la Directiva 95/46/CE con efectos a partir del 25 de mayo de 2018. Además, la plena aplicación del Reglamento General de Protección de Datos implica que hayan de considerarse desplazadas por él aquellas disposiciones de Derecho interno que no resulten conformes con el régimen que el mismo establece. Así sucedería con muchos de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

5.2.1. Objeto del RGPD

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

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

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

5.2.2. Ámbito de aplicación material

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

El RGPD no se aplica al tratamiento de datos personales:

—En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión.

—Por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del titulo V del TUE.

—Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

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

5.2.3. Ámbito territorial

El RGPD amplía el ámbito de aplicación territorial. Se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión Europea, cuando las actividades de tratamiento están relacionadas con la oferta de bienes o servicios o con el control del comportamiento de las personas, si tienen lugar en la UE.

114 Fuente AGPD.

115 Artículo 24 «Responsabilidad del responsable del tratamiento», artículo 25 «Protección de datos desde el diseño y por defecto» y artículo 30 «Registro de las actividades de tratamiento».

5.2.4. Definiciones

El RGPD recoge 26 definiciones, entre las que se contienen varias conocidas y otras nuevas. Destacamos:

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

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Limitación de Tratamiento: El marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

Elaboración de Perfiles: Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

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

Fichero: Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

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

Encargado del tratamiento o encargado: La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Destinatario: La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

Tercero: Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Consentimiento del interesado: Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Violación de la seguridad de los datos personales: Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

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

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

Datos relativos a la salud: Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

5.2.5. Principios

El RGPD, recoge diferentes principios relativos al tratamiento de los datos de carácter personal:

—Principio de *«licitud, lealtad, y transparencia»*. Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado.

—Principio de *«limitación de la finalidad»*. Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. El tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales.

—Principio de *«minimización de datos»*. Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

—Principio de *«exactitud»*. Los datos personales serán exactos, y si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

—Principio de *«limitación del plazo de conservación»*. Los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales. Los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el RGPD a fin de proteger los derechos y libertades del interesado.

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

Estos principios referidos, aunque con denominación diferente, son similares a lo que dispone nuestra normativa.

Además el RGPD recoge el novedoso, principio de *«responsabilidad proactiva»*. Describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD.

5.2.6. Consentimiento

El RGPD define el consentimiento como una manifestación de voluntad, libre, específica e informada e inequívoca, y el responsable del tratamiento de los datos deberá poder probar que el titular «consintió el tratamiento de sus datos personales».

EL RGPD requiere que el interesado preste el consentimiento mediante una declaración inequívoca o una acción afirmativa clara. A efectos del RGPD, el silencio, las casillas ya marcadas, el consentimiento tácito o la inacción no constituirán un consentimiento válido.

Lo más novedoso que aporta el RGPD en las *«Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información»*, es que el consentimiento de los menores solo será válido si tienen más de 16 años. Sin embargo, los Estados miembros de la UE pueden rebajar la edad hasta los 13 años.

5.2.7. La legitimación para el tratamiento de datos personales

El RGPD define el tratamiento como: *«Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción»*.

El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones (bases jurídicas que legitiman el tratamiento):

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

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

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

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

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

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

5.2.8. Tratamiento de categorías especiales de datos personales

El RGPD incluye en el concepto de «categorías especiales de datos personales», los denominados datos especialmente protegidos en la LOPD, como son los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

A estas «categorías especiales de datos personales» el RGPD incorpora: los datos genéticos y datos biométricos, dirigidos a identificar de manera unívoca a una persona física.

5.2.9. Derechos de los interesados

5.2.9.1. Derecho de información de las personas interesadas.

El RGDP establece un nuevo marco normativo de la información. Incluye cuestiones adicionales que actualmente no son requeridas por la normativa española (artículos 13 y 14)[116]. Se refuerza el derecho de información.

La LOPD establece las siguientes obligaciones respecto de la información que se ha de facilitar a las personas interesadas en el momento en que se soliciten los datos:

—La existencia del fichero o tratamiento, su finalidad y destinatarios.

—El carácter obligatorio o no de la respuesta, así como de sus consecuencias.

—La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

—La identidad y datos de contacto del responsable del tratamiento.

El RGPD, añade:

—Los datos de contacto del Delegado de Protección de Datos, en su caso.

—La base jurídica o legitimación para el tratamiento.

—El plazo o los criterios de conservación de la información.

—La existencia de decisiones automatizadas o elaboración de perfiles.

—La previsión de transferencias a Terceros Países.

—El derecho a presentar una reclamación ante las Autoridades de Control.

Y además, cuando los datos no se obtengan del propio interesado, hay que informar de:

—El origen de los datos.

—Las categorías de los datos.

—La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos recae sobre el responsable del Tratamiento.

—La información se debe poner a disposición de los interesados en el momento en que se soliciten los datos, previamente a la recogida o registro, si es que los datos se obtienen directamente del interesado.

En el caso de que los datos no se obtengan del propio interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, el responsable informará a las personas interesadas dentro de un plazo razonable, pero en cualquier caso:

—Antes de un mes desde que se obtuvieron los datos personales.

—Antes o en la primera comunicación con el interesado.

—Antes de que los datos, en su caso, se hayan comunicado a otros destinatarios.

No es preciso informar cuando el interesado ya disponga de la información, ni tampoco, en el caso de que los datos no procedan del interesado, cuando:

—La comunicación resulte imposible o suponga un esfuerzo desproporcionado.

—El registro o la comunicación esté expresamente establecido por el Derecho de la Unión o de los Estados miembros.

—Cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto.

116 Además el RGPD, prevé la transparencia como principio de la protección de datos y como un derecho de las personas (artículo 12).

Por tanto los procedimientos, modelos o formularios diseñados de conformidad con la LOPD deberán ser revisados y adaptados por los responsables de los tratamientos, para cumplir con las nuevas obligaciones que impone este Reglamento.

Se puede consultar la *Guía para el cumplimiento del deber de informar*, publicada por la Agencia Española de Protección de Datos, en su página web.

5.2.9.2. Derechos de Acceso, Rectificación, Cancelación y Oposición.

Los derechos de Acceso, Rectificación, Cancelación y Oposición, ya los establecía la LOPD, los conocidos como ARCO. Se recogen en el RGPD con pequeñas modificaciones.

5.2.9.3. Derecho a la supresión (derecho al olvido).

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

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

b) El interesado retire el consentimiento en que se basa el tratamiento.

c) El interesado se oponga al tratamiento.

d) Los datos personales hayan sido tratados ilícitamente.

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

f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

5.2.9.4. Derecho a la limitación del tratamiento.

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

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

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

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

d) El interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1 del RGPD (derecho de oposición) mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

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

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

5.2.9.5. Derecho a la portabilidad de los datos.

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

a) El tratamiento esté basado en el consentimiento, o en un contrato.

b) El tratamiento se efectúe por medios automatizados.

5.2.9.6. Decisiones individuales automatizadas, incluida la elaboración de perfiles.

Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o que le afecte significativamente en modo similar, salvo que exista consentimiento expreso por parte del titular de los datos, habilitación por normativa europea o de los Estados miembros, o sea necesario para la celebración o ejecución de un contrato entre el interesado y un responsable del tratamiento.

5.2.9.7. Limitaciones al ejercicio de los derechos de los interesados.

En el RGPD se establecen una serie de limitaciones al ejercicio de los derechos de los interesados, cuyo alcance se concreta, en una serie de excepciones al ejercicio de los derechos del Capítulo III del propio RGPD, y de los principios recogidos en el artículo 5, en cuanto se vinculan a dichos derechos.

En el artículo 23 del RGPD se recoge un catálogo de supuestos que justifican las limitaciones al ejercicio de derechos (seguridad del Estado, la defensa, la seguridad pública, etc.).

5.2.10. Contrato de Encargo del tratamiento [117]

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

Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

—Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional.

—Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

117 La Disposición transitoria segunda. Contratos de encargado del tratamiento del Real Decreto-Ley 5/2018, dispone:

«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».

—Tomará todas las medidas de seguridad necesarias.

—Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.

—Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en el RGPD en los artículos 32 a 36[118], teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.

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

—Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el artículo 28 del RGPD, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

Se puede consultar en la página web de la Agencia Española de Protección de Datos la publicación de «Directrices para la elaboración de contratos entre responsables y encargados del tratamiento».

5.2.11. Medidas de responsabilidad activa

5.2.11.1. Análisis del riesgo.

Una de las principales novedades del RGPD, es la realización de un análisis de riesgos relativo al tratamiento de datos.[119]

El RGPD condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados.

De esta forma, algunas de las medidas que el RGPD establece se aplicaran solo cuando el tratamiento suponga un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que el tratamiento presente.

Los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, con el fin de poder establecer qué medidas deben aplicar y como deben hacerlo, teniendo en cuenta entre otros aspectos: tipos de tratamiento, naturaleza de los datos, número de interesados afectados, y la cantidad y la variedad de tratamientos que lleva a cabo una misma organización.

5.2.11.2. Registro de las Actividades de Tratamiento.

Desde el 25 de mayo de 2018, se suprime, la necesidad de crear formalmente los ficheros y notificarlos al Registro de Protección de Datos de las Autoridades de control.

Los responsables de ficheros y/o tratamiento deberán llevar un registro de actividades.

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

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

b) Los fines del tratamiento.

c) Una descripción de las categorías de interesados y de las categorías de datos personales.

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

e) En su caso, las transferencias de datos personales a un tercer país o una organización internacional.

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

g) Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

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

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

b) Las categorías de tratamientos efectuados por cuenta de cada responsable.

c) En su caso, las transferencias de datos personales a un tercer país u organización internacional.

d) Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

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

Las obligaciones indicadas anteriormente, no se aplicaran a ninguna empresa ni organización que emplee a menos de 250 trabajadores, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales, o datos personales relativos a condenas e infracciones penales.

Los tratamientos realizados por las Administraciones Locales se llevarán a cabo mostrando su legitimidad. Se les debe dar publicidad, a través de la página web, sede electrónica o Portal de Transparencia.

5.2.11.3. Protección de datos desde el diseño y por defecto.

Se avanza un paso más para reforzar la responsabilidad proactiva en el cumplimiento normativo. Para ello, el RGPD establece la protección desde el diseño y por defecto.

El responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados.

118 Art. 32 «Seguridad del Tratamiento. Art. 33 «Notificación de una violación de la seguridad de los datos personales a la autoridad de control». Art. 34 «Comunicación de una violación de la seguridad de los datos personales al interesado». Art. 35 «Evaluación de impacto relativa a la protección de datos. Art. 36 «Consulta previa».

119 Se puede consultar la Guía Práctica «Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD», publicada por la Agencia Española de Protección de Datos, en su página web.

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

El responsable del tratamiento que realiza o desea realizar actividades de tratamiento con datos personales, debe establecer procedimientos de control que garanticen cumplir los principios de protección desde el diseño y por defecto.

5.2.11.4. Medidas de seguridad.

El Reglamento de desarrollo de la LOPD, establecía con detalle y de forma exhaustiva las medidas de seguridad que debían aplicarse en función del nivel de seguridad-básico, medio o alto de los datos tratados.

Sin embargo el RGPD que se aplica desde el 25 de mayo de 2018, dispone: «Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) La seudonimización y el cifrado de datos personales.

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

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

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

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

La adhesión a un código de conducta aprobado o a un mecanismo de certificación aprobado, podrá servir de elemento para demostrar el cumplimiento de los requisitos referidos con anterioridad.

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

5.2.11.5. Violación de la seguridad de los datos personales.

Vamos a distinguir:

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

En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

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

La notificación deberá, como mínimo:

—Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

—Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

—Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

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

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

El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

b) Comunicación de una violación de la seguridad de los datos personales al interesado.

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

La comunicación al interesado describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo:

—El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

—Las posibles consecuencias de la violación de la seguridad de los datos personales.

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

La comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

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

—El responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.

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

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

La Agencia Española ha publicado en su página web la *Guía para la gestión y notificación de brechas de seguridad*.

5.2.11.6. Evaluación de impacto relativa a la Protección de Datos.

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

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

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

La consulta debe ir acompañada de la documentación que contempla el RGPD, incluyendo la propia evaluación del impacto, y la autoridad de supervisión puede emitir recomendaciones o ejercer cualquier otro de los poderes que el RGPD le confiere, entre ellos el de prohibir la operación de tratamiento.

La Agencia Española de Protección de Datos ha publicado en su página web la «Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD».

5.2.11.7. El Delegado de Protección de Datos (DPD).

EL RGPD introduce esta nueva figura del Delegado de Protección de Datos, que asume nuevas y cualificadas competencias en materia de coordinación y control del cumplimiento de la normativa de protección de datos.

Esta figura, conocida popularmente como DPO (en inglés, Data Protection Officer), constituye uno de los elementos claves del RGPD, y un garante del cumplimiento de la normativa de la protección de datos en las organizaciones, sin sustituir las funciones que desarrollan las Autoridades de Control.

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

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

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

—las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales o de datos relativos a condenas e infracciones penales.

El RGPD dispone que los delegados de protección de datos sean designados atendiendo a sus cualidades profesionales y, en particular a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos, y su capacidad para el desempeño de sus funciones. No se define en el RGPD el método de evaluación.

La AEPD, ha optado por promover un sistema de certificación de DPD (el candidato deberá justificar la experiencia profesional en materia de protección de datos, así como superar una prueba de evaluación teórica). No obstante, tal certificación es totalmente voluntaria.

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

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

Posición del delegado de protección de datos.

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

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

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

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

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

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

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

—Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud de lo dispuesto en el RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

—Supervisar el cumplimiento de la normativa.

—Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

—Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

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

5.2.12. Códigos de conducta

Los códigos de conducta están destinados a contribuir a la correcta aplicación del RGPD. Es una herramienta de carácter voluntario su adhesión, siendo vinculantes para las instituciones o entidades una vez adheridas al mismo.

El objetivo principal del RGPD al dar una mayor relevancia a los códigos de conducta es que sirvan como herramienta para que los responsables y encargados puedan demostrar el cumplimiento del RGPD.

5.2.13. Mecanismos de certificación

El RGPD promueve los mecanismos de certificación, tales como certificados, sellos o marcas, como mecanismo para demostrar el cumplimiento del RGPD.

5.2.14. Transferencias Internacionales

El en el Capitulo V. Transferencias de datos a terceros países u organizaciones internacionales del RGPD, el artículo 44 dispone: «*Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capitulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado*».

5.2.15. Ventanilla única

Se establece el mecanismo de ventanilla única, que permite que los ciudadanos y también los responsables establecidos en diferentes Estados miembros o que hagan tratamientos que afectan a diferentes Estados miembros tengan una única autoridad de protección de datos como interlocutora.

5.2.16. Recursos, responsabilidad y sanciones

De este apartado destacamos:

—Derecho a presentar una reclamación ante una autoridad de control:

Todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el RGPD.

—Derecho a la tutela judicial efectiva contra una autoridad de control:

Toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

—Derecho a la tutela judicial efectiva contra un responsable o encargado de tratamiento:

Todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del RGPD han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

—Derecho a indemnización y responsabilidad:

Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del RGPD tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el RGPD. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones de RGPD dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

—Condiciones generales para la imposición de multas administrativas:

El artículo 83 del RGPD, describe las condiciones generales para la imposición de multas administrativas:

«1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j).[120]

Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

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

120 Artículo 58.2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

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

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

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

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

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

f) Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.

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

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

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

b) La intencionalidad o negligencia en la infracción.

c) Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados.

d) El grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32.

e) Toda infracción anterior cometida por el responsable o el encargado del tratamiento.

f) El grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción.

g) Las categorías de los datos de carácter personal afectados por la infracción.

h) La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida.

i) Cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas.

j) La adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42.

k) Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10.000.00 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) Las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43 del RGPD.

b) Las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43 del RGPD.

c) Las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4 del RGPD.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) Los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9 del RGPD.

b) Los derechos de los interesados a tenor de los artículos 12 a 22 del RGPD.

c) Las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49 del RGPD.

d) Toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX del RGPD.

e) El incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2 del RGPD, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1 del RGPD.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20.000.000 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable».

—Sanciones:

El artículo 84 del RGPD, dispone:

«Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable».

5.2.17. Autoridades de Control

El RGPD ratifica la obligación que tienen los Estados miembros de crear una autoridad de control.

Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes supervisar la aplicación del RGPD, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

5.2.18. Comité Europeo de Protección de Datos

Se crea el Comité Europeo de Protección de Datos, que sustituye al Grupo de trabajo del artículo 29 de la Directiva 95/46/CE, como organismo de la Unión, que gozará de personalidad jurídica.

El Comité estará representado por su Presidente.

El Comité estará compuesto por el Director de una Autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos.

El Comité actuará con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias con arreglo a los artículos 70 y 71 del RGPD.

La Agencia Española de Protección de Datos en su página web *https://www.agpd.es*, tiene publicadas las siguientes guías:

—Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.

—Guía práctica para las Evaluaciones de Impacto en la Protección de datos sujetas al RGPD.

—Guía del Reglamento General de Protección de Datos para responsables de tratamiento.

—Guía para el cumplimiento del deber de informar.

—Directrices para la elaboración de contratos entre responsables y encargados del tratamiento.

—Guía de Protección de Datos y Administración Local.

—Guía para el ciudadano de Protección de Datos.

—Listado de cumplimiento normativo.

—Guía sobre el uso de las videocámaras para seguridad y otras finalidades.

—Guía para la gestión y notificación de brechas de seguridad.

6. EL PROYECTO DE LEY ÓRGANICA DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

La adaptación al Reglamento General de Protección de Datos, que es aplicable desde 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.

El nuevo texto no trata de ser una nueva Ley para sustituir a la actual LOPD, sino desarrollar el RGPD, para armonizarlo con el resto de la legislación española y, además, para desarrollar algunos puntos que el RGPD deja en manos de los legisladores locales.

El Proyecto de la Ley Orgánica consta de: Exposición de motivos, noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

Los títulos de la Ley son los siguientes:

—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.

—El Título II, recoge los Principios de Protección de Datos:

• Exactitud de los datos.

• Deber de confidencialidad.

• Tratamiento basado en el consentimiento del afectado.

• Consentimiento de los menores de edad.

• Tratamiento de datos amparado por obligación legal, interés público o ejercicio de poderes públicos.

• Categorías especiales de datos.

• Tratamiento de datos de naturaleza penal.

—El Título III, está dedicado a los derechos de las personas:

• Transparencia e información al afectado.

• Ejercicio de los derechos:

• Disposiciones generales sobre ejercicio de los derechos.

• Derecho de acceso.

• Derecho de rectificación.

• Derecho de supresión.

• Derecho a la limitación del tratamiento.

• Derecho a la portabilidad.

vDerecho de oposición.

—El Título IV, recoge las disposiciones aplicables a tratamientos concretos:

• Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.

• Sistemas de información crediticia.

• Tratamientos relacionados con la realización de determinadas operaciones mercantiles.

• Tratamientos con fines de videovigilancia.

• Sistemas de exclusión publicitaria.

• Sistemas de información de denuncias internas.

• Tratamiento de datos en el ámbito de la función estadística pública.

• Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas.

• Tratamiento de datos relativos a infracciones y sanciones administrativas.

—El Título V, se refiere al Responsable y Encargado del Tratamiento:

• Disposiciones generales. Medidas de responsabilidad activa.

• Encargado del tratamiento.

• Delgado de protección de datos.

• Códigos de conducta y certificación.

—El Título VI, es 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 ha 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 «Procedimiento 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.

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.

7. LA VIDEOVIGILANCIA

La imagen de una persona en la medida que identifique o pueda identificar a la misma constituye un dato de carácter personal, que puede ser objeto de tratamiento para diversas finalidades.

La videovigilancia al suponer un tratamiento de datos de carácter personal, salvo que sea de aplicación la denominada excepción doméstica, debe ajustarse a los principios y obligaciones que establece la normativa de protección de datos a los que ya nos hemos referido.

El RGPD establece varios supuestos en su artículo 6 que legitiman el tratamiento de datos de carácter personal, entre los que se encuentra permitir el tratamiento cuando sea necesario para el cumplimiento de una misión de interés público.

Por lo tanto, y puesto que la finalidad de la videovigilancia consiste en garantizar la seguridad de personas, bienes e instalaciones, el interés público legitima dicho tratamiento. Asimismo, el considerando 45 del RGPD contempla que si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público, este tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros.

La captación de imágenes con fines de seguridad, como regla general, de la vía pública debe realizarse por las Fuerzas y Cuerpos de Seguridad. Ya que les corresponde la prevención de hechos delictivos y la garantía de la seguridad en la citada vía pública, de conformidad con lo regulado por la **Ley Orgánica 4/1997, de 4 de agosto**, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, y su Reglamento de desarrollo aprobado mediante Real Decreto 596/1999, de 16 de abril.

Una de las obligaciones que conlleva el uso de la videovigilancia con fines de seguridad, en relación con la protección de datos, es cumplir con el derecho de información, mediante un distintivo informativo.

La AEPD ha publicado en su página web un nuevo cartel de videovigilancia con la finalidad de cumplir con el derecho de información, obligación que impone el RGPD.

Este distintivo se exhibirá en lugar visible, y como mínimo, en los accesos a las zonas vigiladas ya sean interiores o exteriores. En caso que el espacio videovigilado disponga de varios accesos deberá disponerse de dicho distintivo de zona videovigilada en cada uno de ellos.

El distintivo de zona videovigilada deberá informar acerca de:

—La existencia del tratamiento (videovigilancia).

—La identidad del responsable del tratamiento o del sistema de videovigilancia, y la dirección del mismo.

—La posibilidad de ejercitar los derechos reconocidos en los artículos 15 a 22 del RGPD.

—Dónde obtener más información sobre el tratamiento de los datos personales.

—Asimismo, también se pondrá a disposición de los interesados el resto de la información que debe facilitarse a los afectados en cumplimiento del derecho de información regulado en el RGPD.

La AEPD ha publicado en su página web la «Guía sobre el uso de las Videocámaras para Seguridad y otras finalidades».

8. 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

El objeto de este Real Decreto-Ley se ciñe a la adecuación de nuestro ordenamiento al Reglamento Europeo de Protección de Datos en aquellos aspectos concretos que, sin rango orgánico, no admiten demora y debe entenderse sin perjuicio de la necesidad de una legislación orgánica de protección de datos que procure la plena adaptación de la normativa interna a los estándares fijados en la materia por la Unión Europea a través de una disposición directamente aplicable.

Este Real Decreto comprende catorce artículos estructurados en tres capítulos, dos disposiciones adicionales, dos transitorias, una derogatoria y una final. Vamos a analizar los aspectos más relevantes del mismo:

—Capítulo I. Inspección en materia de protección de datos

Atiende a la necesidad de identificar al personal competente para el ejercicio de los poderes de investigación que el Reglamento General de Protección de Datos otorga en su artículo 58.1 a las autoridades de control.

Ello exige que el Derecho interno regule el modo en que podrán ejercerse dichos poderes, qué personas ejercerán la actividad de investigación e inspección y en qué consistirán esas atribuciones expresamente establecidas en el Reglamento Europeo desde el punto de vista del ordenamiento español.

Asimismo, y en aplicación del artículo 62.3 del Reglamento General de Protección de Datos, es preciso determinar el régimen aplicable al personal de las autoridades de supervisión de otros Estados miembros que participen en actuaciones conjuntas de investigación.

Los artículos 1 y 2 de este capítulo se refieren:

a) Ámbito y personal competente para el ejercicio de la actividad de investigación de la Agencia Española de Protección de Datos.

Serán competentes para la actividad de investigación los funcionarios de la Agencia Española de Protección de Datos o funcionarios ajenos habilitados por el Director de la Agencia Española de Protección de Datos. Estos funcionarios tienen la consideración de agentes de la autoridad en el ejercicio de sus funciones.

En los casos de actuaciones conjuntas de investigación conforme a lo dispuesto en el artículo 62 del RGPD, el personal de las autoridades de control de otros Estados Miembros de Unión Europea que colabore con la Agencia ejercerá sus facultades con arreglo a lo previsto en la normativa española y bajo la orientación y en presencia del personal de esta.

b) Alcance de la actividad de investigación.

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. Los poderes de investigación en lo que se refiere a la entrada en domicilios deben ejercerse de conformidad con las normas procesales, en particular, en los casos en los que sea precisa la autorización judicial previa.

—Capítulo II. Régimen Sancionador en materia de protección de datos

Articula el novedoso régimen sancionador establecido en el Reglamento General de Protección de Datos, reemplazando los tipos infractores actualmente contenidos en la Ley Orgánica 15/1999 por la remisión a los que están establecidos en los apartados 4, 5 y 6 del artículo 83 de dicho Reglamento, lo que resulta de todo punto necesario.

Además, existen dos cuestiones sobre las que es ineludible la adopción de disposiciones por el Derecho interno que garanticen la efectividad de este régimen sancionador y la seguridad jurídica en su aplicación:

• La primera se refiere a la necesaria delimitación de los sujetos que pudieran incurrir en la responsabilidad derivada de la aplicación de dicho régimen sancionador.

• La segunda reviste aún mayor importancia y se refiere a la necesidad de determinar los plazos de prescripción de las infracciones y sanciones previstas en la norma europea.

Los artículos 3 a 6 de este capítulo, se refieren:

Sujetos responsables.

Están sujetos al régimen sancionador establecido en el RGPD y en la normativa española de protección de datos:

• Los responsables de los tratamientos.

• Los encargados de los tratamientos.

• Los representantes de los responsables o encargados de los tratamientos no establecidos en la Unión Europea.

• Las entidades de certificación.

• Las entidades acreditadas de supervisión de los códigos de conducta.

No será de aplicación al delegado de protección de datos el régimen sancionador en esta materia.

Infracciones.

Con referencia a las infracciones, este Real Decreto-Ley hace una remisión a las ya recogidas en el RGPD.

De conformidad con el artículo 83.5 del RGPD: «Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000. 000 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

Los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento.

Los derechos de los interesados.

Las transferencias de datos personales a un destinatario en un tercer país o una organización internacional.

Toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capitulo IX.

El incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1».

De conformidad 83.6 del RGPD: «El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20.000. 000 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía».

Las infracciones previstas en los apartados 5 y 6 del artículo 83 del RGPD referidas prescriben a los tres años. 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.

De conformidad con el artículo 83.4: « Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10.000.000 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) Las obligaciones del responsable y del encargado.

b) Las obligaciones de los organismos de certificación.

c) Las obligaciones de la autoridad de control».

Las infracciones previstas en los apartado 4 del artículo 83 del RGPD referidas prescriben a los dos años. 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.

Sanciones.

En cuanto a las sanciones, el Real Decreto-Ley 5/2018, se remite a las contenidas en el RGPD.

Prescripción de las sanciones:

Las sanciones impuestas en aplicación del RGPD 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.

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.

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.

—Capítulo III. Procedimiento en caso de posible vulneración de la normativa de protección de datos

Contiene la regulación del procedimiento en caso de que exista una posible vulneración del Reglamento General de Protección de Datos.

Este último capítulo tiene como objetivo hacer posible la aplicación de las especialidades del régimen procedimental del Reglamento General de Protección de Datos, en un contexto en el que, siendo la norma europea directamente aplicable, ya se han puesto en marcha procedimientos de especial trascendencia al amparo de este régimen.

El artículo 7 del Real Decreto-Ley 5/2018, con referencia al Régimen Jurídico, dispone:

«1. Las disposiciones de este capítulo 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 RGPD, así como en los que aquella investigue la existencia de una posible infracción de lo dispuesto en el mencionado Reglamento y la normativa española de protección de datos.

2. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el RGPD, en la normativa española de protección de datos y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos».

Los artículos 8 al 14 de este capítulo, se refieren a:

—Forma de iniciación del procedimiento y duración.

—Admisión a trámite de las reclamaciones.

—Determinación del alcance territorial.

—Actuaciones previas de investigación.

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

—Medidas provisionales.

—Procedimiento en relación con las competencias atribuidas a la Agencia Española de Protección de Datos por otras Leyes.

—Disposición Adicional Primera. Representación Española en el Comité Europeo de Protección de Datos.

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

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.

—Disposición adicional segunda. Publicación de resoluciones de la Agencia Española de Protección de Datos.

La Agencia Española de Protección de Datos publicará las resoluciones de su Director 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 de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento a las entidades a que se refiere el artículo 46 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, las que impongan medidas cautelares y las demás que disponga su Estatuto.

—Disposición transitoria primera. Régimen transitorio de los procedimientos.

1. Los procedimientos ya iniciados a la entrada en vigor de este Real Decreto-Ley se regirán por la normativa anterior, salvo que el régimen establecido en el mismo 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 segunda. 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.

—Disposición derogatoria única. Derogación normativa.

Quedan derogadas todas las normas de igual o inferior rango que se opongan a lo establecido en el presente Real Decreto-Ley, y en particular, los siguientes artículos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal:

a) El artículo 40.

b) Los artículos 43 al 49, con excepción del artículo 46.

—Disposición final única. Vigencia.

El presente Real Decreto-Ley entrará en vigor al día siguiente de su publicación en el *Boletín Oficial del Estado* y lo estará hasta la vigencia de la nueva legislación orgánica de protección de datos que tenga por objeto 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.

9. PREGUNTAS HABITUALES SOBRE PROTECCIÓN DE DATOS

1. ¿Desde cuando se aplica el nuevo Reglamento General de Protección de Datos (RGPD)?

EL RGD se aplica desde el 25 de mayo de 2018.

2. ¿Qué es un dato de carácter personal?

Toda información sobre una persona física identificada o identificable («el interesado»). Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (Definición del Reglamento General de Protección de Datos).

3. ¿Quién es el Responsable del tratamiento y el Encargado del tratamiento?

El Responsable del tratamiento o responsable es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros (Definición del RGPD).

El Encargado del tratamiento o encargado es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (Definición del RGPD).

4 ¿Qué es un tratamiento?

Es cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción(Definición del RGPD).

5 ¿Cuáles son los principios de la protección de datos, según el RGPD?

—Principio de «licitud, lealtad, y transparencia».
—Principio de «limitación de la finalidad».
—Principio de «minimización de datos».
—Principio de «exactitud».
—Principio de «limitación del plazo de conservación».
—Principio de «integridad y confidencialidad».
—Principio de «responsabilidad proactiva».

6. ¿Qué derechos nuevos incorpora el Reglamento a los establecidos en la LOP?

A los derechos que ya establecía la LOPD: Acceso, Rectificación, Cancelación y Oposición, los conocidos como ARCO, se contemplan:

—Derecho a la supresión (derecho al olvido).
—Derecho a la limitación del tratamiento.
—Derecho a la portabilidad de los datos.
—El derecho a no ser objeto de una elaboración de perfiles.

7 ¿Cuál es el procedimiento para el ejercicio de los derechos recogidos en el nuevo RGPD?

Los responsables deben facilitar a los interesados el ejercicio de sus derechos. Los procedimientos y las formas para ello deben ser visibles, accesibles y sencillos. Los responsables deben posibilitar la presentación por medios electrónicos, especialmente cuando el tratamiento se realiza por este medio.

8. Según el RGPD ¿cómo debe solicitarse el consentimiento de los interesados para tratar sus datos personales?

Una de las bases fundamentales para tratar los datos personales es el consentimiento. El RGPD requiere que el consentimiento sea «libre, informado, específico e inequívoco».

Se debe prestar mediante una manifestación del interesado o mediante una clara acción afirmativa. El consentimiento no puede deducirse del silencio o de la inacción de los ciudadanos.

9. ¿Qué obligaciones propias tienen los Encargados del tratamiento?

Deben mantener un registro de actividades del tratamiento, determinar las medidas de seguridad aplicables a los tratamientos que realizan y designar a un Delegado de Protección de Datos en los casos previstos por el RGPD.

Además pueden adherirse a códigos de conducta o certificarse en el marco de los esquemas de certificación previstos por el RGPD.

10. En el ámbito de la Administración Local, ¿qué base jurídica legitima los tratamientos?

La base jurídica que legitima los tratamientos será el cumplimiento de una tarea de interés público o el ejercicio de poderes públicos, así como el cumplimiento de una obligación legal. En ambos casos, debe existir una previsión normativa de Ley.

11. El principio de responsabilidad activa del RGPD ¿en qué consiste?

El RGPD establece un catálogo de las medidas que los responsables, y en ocasiones los encargados, deben aplicar para garantizar que los tratamientos son conformes al citado RGPD, así como que están en condiciones de demostrarlo.

Estas medidas de responsabilidad activa son las siguientes:

—Análisis de riesgo.
—Registro de actividades del tratamiento.
—Protección de datos desde el diseño y por defecto.
—Adopción de medidas de seguridad.
—Notificación de «violaciones de seguridad de los datos»
—Evaluaciones de impacto sobre la protección de datos.
—Nombramiento del Delegado de Protección de Datos.

12. ¿En qué consiste el análisis de riesgo al que se refiere el RGPD?

El RGPD prevé que las medidas de cumplimiento para responsables o encargados deban aplicarse en función del riesgo que los tratamientos que realizan supongan para los derechos y libertades de los interesados.

Por ello, responsables y encargados deben llevar a cabo una valoración del riesgo de los tratamientos que realicen, con el fin de determinar qué medidas aplicar y cómo hacerlo.

Este análisis del riesgo variará en función de:

—Los tipos de tratamiento.
—La naturaleza de los datos.
—El número de interesados afectados.
—La cantidad y variedad de tratamientos.

13. ¿Se puede seguir aplicando con el RGPD las mismas medidas que con el Reglamento de la LOPD?

A diferencia del Reglamento de desarrollo de la LOPD, el RGPD no contempla un listado de medidas de seguridad en función de si el tipo de tratamientos es de nivel bajo, medio o alto, de forma que desde el 25 mayo de 2018, que es aplicable el RGPD, este listado no será válido de forma automática.

En algunos supuestos se podrá seguir aplicando las mismas medidas que establece el Reglamento de la LOPD si los resultados del análisis de riesgos previo concluyen que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado. En ocasiones será necesario completarlas con medidas adicionales o prescindir de ellas.

14. ¿Qué pasos realizará un Ayuntamiento para adaptarse al RGPD?

—Designar un Delegado de Protección de Datos.
—Elaborar un Registro de Actividades de Tratamiento.
—Identificación con precisión de las finalidades y de las bases jurídicas de los tratamientos que se llevan a cabo.
—Revisar la información que se ofrece a los interesados cuando se recogen sus datos a las exigencias del RGPD.
—Revisar los procedimientos de los ejercicios de los derechos de los interesados.
—Revisar los contratos realizados con los Encargados de Tratamiento.
—Establecer y revisar los procedimientos para acreditar el consentimiento.
—Efectuar Análisis de Riesgos para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que se lleven a cabo.
—Revisar las medidas de seguridad que se aplican a los tratamientos a luz de los resultados del análisis del riesgo de los mismos.
—Necesidad de establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos y reaccionar ante ellas.
—Determinar la necesidad de efectuar evaluaciones de impacto en la protección de los datos sujetas al RGPD.
—Adaptar los instrumentos de Transferencia Internacional de datos personales a las previsiones del RGPD.
—Elaborar y llevar a cabo un Plan de formación y concienciación de los empleados públicos, y cargos públicos.

La Agencia Española de Protección de datos, ha lanzado un listado de cumplimiento normativo para facilitar la adaptación del RGPD, que se puede consultar en su página web.

15. ¿Quién es el Delegado de protección de datos (DPD)?

EL RGPD introduce esta nueva figura del Delegado de Protección de Datos, que asume nuevas y cualificadas competencias en materia de coordinación y control del cumplimiento de la normativa de protección de datos.

El RGPD establece que el DPD, será designado, atendiendo a sus cualidades profesionales y, en particular a sus conocimientos especializados del Derecho, y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que el RGPD le atribuye.

16. ¿Se pueden instalar cámaras de videovigilancia que graben la vía pública?

Sí; pero hemos de tener en cuenta que la instalación de videocámaras en lugares públicos, tanto móviles como fijos, es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad del Estado, rigiéndose el tratamiento de dicha imágenes por su legislación específica, contenida en la Ley Orgánica 4/1997, de 4 de agosto, y su Reglamento de desarrollo, sin perjuicio de que les sea aplicable, en su caso, lo previsto por el RGPD, en aspectos como la adopción de las medidas de seguridad que resulten de aplicación y la elaboración del registro de actividades en relación con el tratamiento de videovigilancia que se realice.

17. ¿Quiénes están sujetos al régimen sancionador establecido en el RGPD y en la normativa española de protección de datos?

Están sujetos:

—Los responsables de los tratamientos.

—Los encargados de los tratamientos.

—Los representantes de los responsables o encargados de los tratamientos no establecidos en la Unión Europea.

—Las entidades de certificación.

—Las entidades acreditadas de supervisión de los códigos de conducta.

No será de aplicación al delegado de protección de datos el régimen sancionador en esta materia.

18. ¿Se podrán imponer las multas administrativas del RGPD a las Entidades Locales?

Según el RGPD, corresponde a los Estados miembros determinar si, y en que medida, se deben imponer multas a las autoridades públicas. En nuestra normativa no se estable la posibilidad de imponer multas a las Administraciones Locales.