# LA NUEVA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS

ROSA MARÍA GARCÍA PÉREZ

*Profesora Titular de Derecho civil. Delegada de Protección de Datos. Universidad de Granada*[1]

## SUMARIO:



## I. EL DELEGADO DE PROTECCIÓN DE DATOS, UNA FIGURA OBLIGATORIA EN EL MODELO DE GESTIÓN DE DATOS PERSONALES EN LAS ADMINISTRACIONES PÚBLICAS

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 (Reglamento General de Protección de Datos, en adelante, RGPD) establece un marco jurídico común en la Unión Europea de protección de datos de carácter personal, dirigido a garantizar de una manera uniforme el derecho a la privacidad de las personas así como la libre circulación de los datos. En España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) ha completado y adaptado las previsiones generales de la norma europea en el ámbito nacional, dentro del límite del margen de apreciación que el RGPD concede a los Estados miembros. Al mismo tiempo, se ha utilizado la norma nacional para integrar en nuestro Ordenamiento un marco de reconocimiento y protección de los denominados "derechos digitales".

[1]Ponencia presentada a la Jornada de Excelencia sobre la Nueva figura del Delegado de Protección de datos organizada por el CEMCI el 10 de octubre de 2019.

El RGPD es una norma aplicable cualquiera que sea el contexto en el que opera el responsable del tratamiento, por ello afecta no sólo a los tratamientos de datos personales por sujetos privados, sino también de manera frontal a las Administraciones Públicas en cuanto responsables de múltiples tratamientos en sus relaciones con los ciudadanos.

La incidencia del RGPD en este punto es fundamental al cambiar sustancialmente, respecto de la normativa anterior, la manera en que se deben garantizar los derechos y cumplir esas obligaciones. Ello es debido fundamentalmente a la proclamación de un nuevo principio presente en todo el articulado del texto legal. Se trata del principio de responsabilidad proactiva que exige, a cualquier entidad u organización que trate datos personales, conocer el régimen jurídico de la protección de datos, realizar una valoración previa sobre la afectación o riesgos a la privacidad que tales tratamientos puedan comportar, y adoptar las medidas que procedan para evitarlos. Se adopta un modelo en el que cada responsable del tratamiento ha de demostrar que conoce sus obligaciones y, en base a ello, adopta las oportunas decisiones técnicas y organizativas.

Los cambios que se introducen como consecuencia de la aplicación de este principio afectan desde el inicio de cualquier tratamiento de datos personales, durante el ciclo de vida del mismo y una vez concluido; a título ilustrativo pueden citarse entre tales cambios los siguientes: la desaparición del registro de ficheros en la Agencia Española de Protección de datos (en adelante, AEPD), la obligación de realizar análisis de riesgos y evaluaciones de impacto en determinados tratamientos, la obligatoriedad de asumir la privacidad por diseño y por defecto, el establecimiento de medidas técnicas y organizativas de seguridad apropiadas…

En todo el proceso de adaptación, la figura del Delegado de Protección de Datos (en adelante, DPD), obligatoria en las Administraciones Públicas, desempeñará un papel fundamental de información y asesoramiento a la entidad responsable en la implementación de las medidas de cumplimiento normativo, y de supervisión y garantía de derechos.

Conviene, no obstante, saber que el marco de la privacidad en Europa incluye, omitiendo otras normas sectoriales, además:

- La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Esta Directiva extiende la regulación de la protección de datos a los ámbitos de la cooperación judicial en materia penal y de la cooperación policial.
- Y, en un futuro no muy lejano, el Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se

deroga la Directiva 2002/58/CE, conocido como Reglamento sobre la privacidad en las comunicaciones electrónicas o Reglamento *E-Privacy*, cuya propuesta fue presentada por la Comisión europea el pasado 10 de enero de 2017, y actualmente se está discutiendo en el Consejo de la Unión Europea, tras su paso por la Comisión y el Parlamento.

Afectará fundamentalmente a la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI) y tendrá una gran incidencia en el ámbito de comunicaciones bajo el *Internet Protocol*. A diferencia del RGPD cuyo ámbito de protección queda circunscrito a las personas físicas, en el marco de la protección otorgada por la Carta de los Derechos Fundamentales de la UE (arts. 7 y 8), la protección que ofrecerá el Reglamento E-Privacy se extenderá a las personas jurídicas, que no están bajo el ámbito de la Carta.

## 2.. CLAVES PARA LA COMPRENSIÓN DEL NUEVO RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN PÚBLICA

### 2.1. El Reglamento General de Protección de Datos. Su impacto en la Administraciones Públicas

Tal y como he recogido en un trabajo anterior[2], a mi modo de ver las claves del nuevo modelo de gestión de los datos personales implementado por el RGPD, para cualquier entidad u organización, pasan por las siguientes consideraciones:

#### A- Homogeneización y armonización, no sólo a nivel europeo

El RGPD amplia el alcance territorial de la normativa europea en materia de protección de datos, dando solución a problemas de ley aplicable y jurisdicción que, especialmente, habían planteado las grandes corporaciones internacionales que operan en los Estados miembros y son responsables de tratamientos de datos personales pero carecen de sede en la Unión Europea, tal es el caso de entidades titulares de redes sociales, aplicaciones informáticas, motores de búsqueda, servicios de computación en nube… Significativa en este sentido es la cuestión prejudicial planteada por la Audiencia Nacional al Tribunal de Justicia de la Unión Europea por Auto de 27 de febrero de 2012 en el caso Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos, Mario Costeja González[3] y resuelta por el Tribunal de Justicia

[2] Rosa María GARCÍA PÉREZ, "La protección de datos de carácter personal del consumidor en el mercado único digital, Revista de Derecho Mercantil Nº 301, julio-septiembre 2016, págs. 199-251

[3] Las dudas de la Audiencia Nacional en este ámbito se centraban, en primer lugar, en concretar si cuando el proveedor de un motor de búsqueda responsable del tratamiento es una sociedad establecida fuera de la Unión Europea —como sería el caso de Google Inc— cabe considerar que tiene un «establecimiento» en España a los efectos de que le sea aplicable la legislación española sobre protección de datos cuando tiene en España una filial —como sería el caso de Google Spain, S.L.— para la promoción y venta en España de los espacios publicitarios del buscador. Así como, en segundo lugar, la interpretación del criterio del «recurso a medios situados en el territorio de dicho Estado miembro» como determinante de la aplicación de la legislación europea y española de protección de datos; se solicitaba saber si tal circunstancia concurre en un Estado miembro en el que se encuentran servidores que alojan páginas web que contienen información, objeto de localización e indexación por el motor de búsqueda (lo que resulta determinante de que la información alojada en servidores situados en España pueda aparecer referenciada en los resultados del buscador) o cuando el buscador en cuestión utiliza un nombre de dominio propio de un Estado miembro —como sucede con «.es»-

europeo en sentencia de 13 de mayo de 2014 (asunto C-131/2012)[4].

La nueva normativa europea será aplicable a aquellos responsables de tratamientos de datos que, aún no teniendo un establecimiento en Europa, dirijan sus ofertas de bienes o servicios a ciudadanos de la Unión, independientemente de que requieran o no el pago de una contraprestación, o monitoricen sus conductas (artículo 3 del Reglamento), en el sentido expresado en el considerando 24 del Reglamento, conforme al cual «para determinar si se puede considerar que una actividad de tratamiento "controla la conducta" de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet con técnicas de tratamiento de datos que consistan en la elaboración de un perfil de un individuo con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes».

La articulación de un marco normativo homogéneo se ve asimismo favorecida por la introducción de un sistema de "ventanilla única" o "*one-Stop-shop solution*" y el fortalecimiento de la eficacia e independencia de las autoridades nacionales de control, tanto en sus funciones como en la potestad que se les confiere de imponer importantes sanciones económicas, al tiempo que se establecen mecanismos que su cooperación activa y coherencia en la aplicación de la protección de datos personales en la Unión Europea.

El enfoque "*one-stop-shop*" (art. 56) implica, para las personas titulares de los datos, hacer valer sus derechos con facilidad ante su autoridad nacional de protección de datos y en su propia lengua, aun cuando sus datos se traten fuera de su país de origen. Igualmente, las entidades u organizaciones sólo tendrán que acudir a la autoridad competente del país en el que tengan su sede central, lo que simplifica y abarata operar en toda la Unión Europea.

La cooperación entre las autoridades de control se basa en dos pilares, la asistencia mutua, a fin de aplicar el presente Reglamento de manera coherente (artículo 61), y la posibilidad de que realicen operaciones conjuntas en investigaciones o para hacer un seguimiento de la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro (artículo 62). Junto con estas medidas se contempla el denominado mecanismo de coherencia (artículo 63), que «debe aplicarse en particular cuando una autoridad de control pretenda adoptar una medida concebida para surtir efecto jurídico en lo que se refiere a operaciones de tratamiento que afecten sustancialmente a un número significativo de interesados en varios Estados miembros). También debe aplicarse cuando cualquier autoridad de control *afectada* o la Comisión soliciten que dicho asunto se trate en el marco del mecanismo de coherencia» (considerando 135).

[4] El Tribunal de Justicia de la Unión Europea consideró que el tratamiento de datos personales realizado por el motor de búsqueda Google Search, gestionado por una empresa que tiene su domicilio social en EEUU pero que crea en un Estado miembro una sucursal o filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro, se efectúa «en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro». el Tribunal no entra analizar si concurren o no en el caso concreto los demás puntos de conexión previstos en el artículo 4 de la Directiva 95/46.

## B. "Apoderar" a la persona en relación con sus datos personales y sus derechos

Cualquier tratamiento de datos debe estar basado en una causa o base legal contemplada en el artículo 6 RGPD:

a) el interesado presta el consentimiento para el tratamiento de su información personal

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.»

En el ámbito de las administraciones públicas, para la justificación de los tratamientos que realizan tendrán especial relevancia las causas mencionadas en los apartados c) y e), esto es, el cumplimiento de una obligación legal o de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, fundamentalmente porque el consentimiento, que tradicionalmente ha sido el primer fundamento legitimador de todo tratamiento de datos personales, ha perdido peso en este ámbito como consecuencia de la contundencia y refuerzo de sus caracteres imprimidos por el RGPD. Así se exige:

a. **Consentimiento libre.** La validez del consentimiento requiere la ausencia de vicio. El artículo 7 del Reglamento incide en este atributo de dos formas:

Por una parte, indicado en su apartado 2 que, si el consentimiento del interesado se ha de dar en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento deberá presentarse de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo; aspectos estos últimos de accesibilidad y calidad de la presentación que entroncan con el principio de transparencia de la información (art. 12 RGPD). Habrá, pues, falta de libertad cuando no se permita dar consentimiento por separado a las distintas operaciones de tratamiento de datos pese a ser lo adecuado en ese caso concreto (considerando 43 RGPD).

Por otra, al señalar, en su apartado 4, que para evaluar si el consentimiento se ha otorgado libremente se tendrá en cuenta el hecho de que la ejecución de un contrato, o la prestación de un servicio, se haya condicionado a la autorización de un tratamiento de

datos que no sea necesario para el cumplimiento del mencionado contrato. El considerando 43, recogiendo esta idea, va más allá al precisar que, para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido en un caso particular cuando exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando el responsable es una autoridad pública y es poco probable que el consentimiento se haya dado libremente en todas las circunstancias de esa situación específica.

b. **Consentimiento específico**, lo que supone la concreción de los fines, que deben ser explícitos y legítimos, para los que se recaban los datos, sin que puedan ser tratados posteriormente de manera incompatible con dichos fines (principio de limitación de los fines).

c. **Consentimiento informado**. Este carácter guarda estrecha relación con los principios de licitud, lealtad y transparencia (art. 5.a. RGPD) y supone la exigencia de que, antes de la emisión del consentimiento, se cuente con información exacta y completa sobre la identidad del responsable, los fines del tratamiento, el plazo de conservación de los datos y demás extremos recogidos en el artículo 13 RGPD.

d. **Consentimiento inequívoco.** El RGPD exige su manifestación mediante una declaración o una clara acción afirmativa, por lo que no cabe el consentimiento por omisión o inacción.

En esta misma línea de "empoderar" al ciudadano y permitirle un mayor control sobre sus datos, se refuerzan los tradicionales derechos ARCO (acceso, rectificación, cancelación y oposición) y aparecen nuevos derechos.

- El denominado derecho a la supresión o **«derecho al olvidado»** (artículo 17 RGPD)[5], cuyo objeto es evitar que datos e informaciones que su titular considera dañinos para su privacidad puedan perpetuarse en internet. Permite a cualquiera exigir del responsable del tratamiento que suprima inmediatamente los datos personales cuando:
    - Los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados.
    - El interesado retira el consentimiento en que se basa el tratamiento, o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos.
    - El interesado se opone al tratamiento de datos personales, por motivos relacionados con su situación particular, salvo que el responsable del tratamiento acredite motivos imperiosos y legítimos que prevalezcan sobre los intereses o los derechos y libertades fundamentales del interesado.

[5] .- Tema del que me he ocupado ampliamente, vid. GARCÍA PÉREZ, Rosa María, "Privacidad y derecho al olvido digital. El caso español", en *Constitución, Derecho y derechos*, coord. por Giovanni PRIORI POSADA, ed. Palestra. Lima, Perú, 2016, págs. 77 a 108.

- Los datos deban suprimirse para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento.
- El tratamiento de datos es ilícito.

Este derecho comporta también, para los responsables del tratamiento que hayan hecho públicos los datos personales, la obligación de a informar a los responsables del tratamiento que estén tratando tales datos de que supriman todo enlace, las copias o réplicas de tales datos.

No obstante, se prevén excepciones basadas en el derecho a la libertad de expresión, en motivos de interés público en el ámbito de la salud pública, en fines de archivo de interés público o fines de investigación histórica, estadística y científica, en el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o por venir impuesto como obligación legal de conservar los datos personales por el Derecho aplicable, sea el comunitario o el del Estado miembro a que esté sujeto el responsable del tratamiento.

- **Derecho a la limitación-restricción del tratamiento.** El interesado tendrá derecho a obtener del responsable la limitación del tratamiento de sus datos personales cuando: a) el interesado impugne la exactitud de los datos, durante un plazo que permita al responsable del tratamiento 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 a limitación de su uso; c) el responsable del tratamiento ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; o d) el interesado se ha opuesto al tratamiento conforme al artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable del tratamiento prevalecen sobre los del interesado (artículo 18 Reglamento).

Indica el considerando 67 que «entre otros métodos para restringir el tratamiento de datos personales podrían incluirse los consistentes en trasladar los datos seleccionados a otro sistema de tratamiento, o impedir el acceso de usuarios a los datos seleccionados, o retirar temporalmente los datos publicados de un sitio internet».

- **Derecho a la portabilidad** consistente en la posibilidad que tiene el titular de los datos personales, por un lado, de obtener una copia de dichos datos en un formato electrónico comúnmente utilizado; y, por otro lado, de transferir dichos datos si la tecnología lo permite a otros responsables de tratamiento, siempre y cuando el tratamiento de sus datos se efectúe por medios automatizados y se base en el consentimiento o en el cumplimiento de un contrato (artículo 20 RGPD). Esta nueva facultad pretende, pues, facilitar la transmisión de datos personales de un proveedor de servicios, a otro, promoviendo la competencia entre estos.

- Especial mención requiere el **derecho a oponerse a una** decisión individual automatizada, incluida la elaboración de perfiles **a la elaboración de perfiles** previsto en el artículo 22 RGPD. Se trata de poner límites a los resultados que se puedan obtener a partir de técnicas automatizadas de explotación de datos masivos. Así se consagra el derecho a no ser objeto de una evaluación sistemática y

exhaustiva de los aspectos personales que puedan generar un perfil del individuo sobre el que se puedan tomar decisiones que tengan, especialmente, efectos discriminatorios o le afecten jurídicamente.

No obstante, como señala el considerando 71 y resulta del propio artículo 22 del Reglamento, «se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de observación y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito».

En cualquier caso, el tratamiento de datos personales basado en la elaboración de perfiles es sometido por el Reglamento a ciertas cautelas, fundamentalmente, informar adecuadamente al interesado de este tipo de tratamiento con sus datos personales (artículo 14) e imponer al responsable la realización de una evaluación de impacto (artículo 35.3.a), así como objeto de sanciones agravadas impuestas por la autoridad de control en el supuesto de incumplimiento de las previsiones legales (artículo 83).

- **Derecho a ser informado de cualquier brecha de seguridad** que pueda suponer un alto grado de riesgo para sus derechos y libertades de las personas, por ejemplo problemas de discriminación, usurpación de identidad o fraude, pérdidas económicas, menoscabo de la reputación, cambio no autorizado de la seudonimización, pérdida de confidencialidad de datos sujetos al secreto profesional o cualquier otro perjuicio económico o social significativo.

Esta obligación de informar sobre posibles fugas de información o *data breach notification* ya existe en el ámbito de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas), que establece que los proveedores de servicios de comunicaciones electrónicas tienen la obligación de informar a las autoridades de control, y en algunos supuestos a los propios abonados, de las quiebras de seguridad de los datos personales de los abonados. Por su parte, el Reglamento (UE) 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE, fija las normas sobre cómo y cuándo notificar estas quiebras de seguridad.

El Reglamento prevé que el responsable del tratamiento comunique al interesado, sin demora injustificada, la violación de sus datos personales (artículo 34 RGPD). Igualmente estará obligado a notificarla a la autoridad de control competente, sin demora injustificada y, a ser posible, no después de las 72 horas siguientes (artículo 33 RGPD).

## C. Prevención antes que reacción: una adecuada y responsable gestión de los riesgos a través una cultura institucional de la protección datos

El RGPD establece también mecanismos de prevención, que implementan en las entidades y organizaciones toda una cultura de protección de datos, a través de la introducción de los conceptos de privacidad por defecto y desde el diseño; del análisis de riegos o evaluación de impacto; de la figura del Delegado de Protección de Datos; de la responsabilidad; y de la certificación. A continuación se analizarán brevemente cada uno de estos mecanismos para centrar la siguiente parte en el Delegado de Protección de Datos (DPD).

### a. Privacidad desde el diseño y por defecto

El RGPD viene a reforzar el actual principio de calidad de los datos conforme al cual los datos para el tratamiento deben ser adecuados, pertinentes y no excesivos, al establecer la necesidad, por parte del responsable del tratamiento, tanto con carácter previo al tratamiento de datos que se quiera realizar como durante el tratamiento, de adoptar medidas de carácter técnico u organizativo que minimicen el número de datos personales tratados y aseguren que, por defecto, sólo se tratarán los datos personales imprescindibles y necesarios para cada objetivo o finalidad específica del tratamiento.

*Artículo 25. Protección desde el diseño y por defecto*

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

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

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

La privacidad desde el diseño busca, como se indicado gráficamente, "encastrar" desde el origen la privacidad en sus productos, servicios, procedimientos administrativo o prácticas de negocio, sistemas de información, arquitecturas y redes de comunicación, implementando además mecanismos dirigidos a garantizar que, por defecto, su

configuración recoge las opciones menos intrusivas y más protectoras de la privacidad para los usuarios.

### b. Evaluaciones de impacto

La evaluación de impacto de la privacidad o *privacy impact assesment* (en sus siglas inglesas, PIA), como mecanismo de prevención de riesgos, constituye en el RGPD una obligación impuesta a los responsables de ciertos tratamientos de datos, quienes deberán, antes de iniciar el tratamiento, evaluar si este provocará o no daños a los derechos y libertades de los interesados (como, por ejemplo, problemas de discriminación, usurpación de identidad o fraude, pérdidas económicas, menoscabo de la reputación, cambio no autorizado de la seudonimización, pérdida de confidencialidad de datos sujetos al secreto profesional o cualquier otro perjuicio económico o social significativo) y, en su caso, tomar las medidas que consideren apropiadas para prevenir y evitar dichos daños.

El artículo 35 RGPD enumera una serie de tratamientos que, por entender que siempre entrañan riesgos, exigirán realizar una evaluación de impacto:

a. La evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en la elaboración de perfiles y sobre la base de la cual se tomen decisiones que produzcan efectos jurídicos en relación con los interesados o que les afecten gravemente;

b. El tratamiento a gran escala de las categorías especiales de datos personales a que se refiere el artículo 9, apartado 1 (información sobre la vida sexual, la salud, la raza y el origen étnico) o de datos sobre condenas o infracciones penales a que se refiere el artículo 10 del Reglamento;

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

Asimismo, el Reglamento autoriza a la autoridad nacional de control a establecer listados de operaciones de tratamiento que deberán ir precedidos de la correspondiente evaluación de impacto y de aquellas para las que no se requiere, debiendo en todo caso comunicarlos al Comité Europeo de Protección de Datos (apartados 4 y 5 del artículo 35 del Reglamento).

La primera consecuencia de estas evaluaciones es que desaparece la tradicional clasificación de niveles de seguridad en el tratamiento de datos personales y las medidas de seguridad se tendrán que implantar en función del peligro que genere el impacto de dicho tratamiento.

La evaluación deberá incluir, como mínimo, una descripción general de las operaciones de tratamiento previstas, una valoración del riesgo, las medidas contempladas para hacer frente al riesgo, con inclusión de garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos personales y a probar la adecuación a la normativa vigente (art. 35.7).

### c. Códigos de conducta y certificación

Se reconoce la posibilidad de otorgar validez general dentro de la Unión Europea a los códigos de conducta sometidos a examen de la Comisión que, al tiempo de servir como mecanismo de verificación del cumplimiento de determinadas obligaciones impuestas por la normativa, podrán constituir garantía adecuada en el marco de las transferencias internacionales de datos ofrecida por responsables o encargados de tratamiento de terceros países que se adhieran a ellos. Los Códigos, conforme a lo dispuesto por el artículo 40 RGPD, serán promovidos por los Estados Miembros, las autoridades de control, el Comité Europeo de Protección de Datos y la Comisión, atendiendo a las peculiaridades de cada sector y de las pequeñas y medianas empresas. Si el tratamiento objeto del código afecta a un solo Estado Miembro, será la autoridad de control de ese Estado la encargada de supervisarlo, imponer las salvaguardas adecuadas, registrarlo y publicarlo. Pero si afecta a varios Estados, el encargado de supervisarlo y enmendarlo será el Comité Europeo de Protección de Datos, que posteriormente dará traslado del mismo a la Comisión Europea para que declare en su caso, su validez en toda la Unión y lo publique.

Se trata de instrumentos de autorregulación que suponen un valor añadido, tanto en la esfera interna o sectorial como desde la perspectiva de los consumidores, en cuanto que complementan o especifican la aplicación de la normativa general al concreto sector o ámbito. En este sentido, a título ilustrativo, el artículo 40.2 RGPD indica que podrán concretar la aplicación de la normativa en cuestiones tales como: a) el tratamiento leal y transparente de los datos; b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos; c) la recogida de datos personales; d) la seudonimización de datos personales; e) la información proporcionada al público y a los interesados; f) el ejercicio de los derechos de los interesados; g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de os titulares de la patria potestad o tutela sobre el niño; h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32; i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados; j) la transferencia de datos personales a terceros países u organizaciones internacionales, o k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79. Asimismo, se advierte que los códigos deberán incorporar mecanismos que permitan al órgano de supervisión o control, llevar a cabo el control obligatorio del cumplimiento de las disposiciones del código.

La norma europea configura también un sistema de certificación europeo en materia de protección de datos con la finalidad de «aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación, sellos y marcas de protección de datos, que permitan a los interesados evaluar más rápidamente el nivel de protección de datos de los productos y servicios correspondientes» (considerando 100).

De este aspecto se ocupan los artículos 42 y 43 del Reglamento referentes a la certificación y al organismo y procedimiento de certificación, respectivamente,

encomendando a los Estados miembros, las autoridades nacionales de control, el Comité Europeo de Protección de Datos y a la Comisión promover la creación de estos mecanismos de certificación.

Se otorga potestad, a las autoridades de control nacionales y a organismos de certificación debidamente acreditados, de emitir certificaciones o sellos de protección de datos, cuya validez será de 3 años (renovable), a entidades que voluntariamente se sometan a procesos de certificación y garantizarán que el tratamiento de datos personales se efectúa de conformidad con la normativa.

La existencia de este tipo de sellos o distintivos facilita la acreditación por parte del responsable del tratamiento de que éste se lleva de conformidad con la normativa (artículo 24.3 del Reglamento), al tiempo que se convertirá en una ventaja competitiva para las empresas y entidades, al permitir a los consumidores identificar fácilmente si se cumplen las normas en el tratamiento de sus datos, siendo especialmente relevante para las entidades que se plantean externalizar parte de sus procesos o servicios en los que se traten datos de carácter personal (*cloud computing*) o para las que pretendan operar fuera del ámbito europeo ampliando su mercado, dado que serán un instrumento adecuado, en los supuestos de transferencias internacionales de datos, para acreditar que se ofrecen garantías suficientes y apropiadas de protección (artículo 42.2 del Reglamento).

Se encomienda al Comité Europeo de Protección de Datos recopilar en un registro todos los mecanismos de certificación y sellos de protección de datos y ponerlos a disposición del público a través de cualquier medio adecuado, como por ejemplo el portal europeo de justicia (https://e-justice.europa.eu/).

### D. Impacto del RGPD en Administraciones Publicas

Según resulta del documento publicado por la Agencia Española de Protección de Datos, relativo al "El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Publicas", las principales consecuencias, además de designar un DPD, son las siguientes:

a. Necesidad de identificar con precisión las finalidades y la base jurídica de los tratamientos que llevan a cabo
b. Necesidad de adecuar la información que se ofrece a los interesados cuando se recogen sus datos a las exigencias del RGPD (arts. 13 y 14).
c. Necesidad de establecer mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos, para el ejercicio de derechos.
d. Necesidad de establecer procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD.
e. Necesidad de valorar si los encargados con los que se hayan contratado o se vayan a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD.
f. Necesidad de adecuar los contratos de encargo que actualmente se tengan suscritos a las previsiones del RGPD.

g. Necesidad de hacer un análisis de riesgo para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que se desarrollen.

h. Necesidad de establecer un Registro de Actividades de Tratamiento.

i. Necesidad de revisar las medidas de seguridad que se aplican a los tratamientos a la luz de los resultados del análisis de riesgo de los mismos.

j. Necesidad de establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos y reaccionar ante ellas, en particular para evaluar el riesgo que puedan suponer para los derechos y libertades de los afectados y para notificar esas violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados.

k. Necesidad de valorar si los tratamientos que se realizan requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados y de disponer de una metodología para llevarla a cabo.

l. Necesidad de adaptar los instrumentos de transferencia internacional de datos personales a las previsiones del RGPD.

## 2.2. Incidencia de la Ley Orgánica de Protección de Datos y garantía de los derechos digitales en el sector público

Como se advierte en la Exposición de Motivos de la LOPDGDD, el RGPD no **"**excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico", de ahí la necesidad de adoptar una nueva Ley que sustituya a la anterior Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales.

Las principales novedades de la norma para el sector público han sido recogidas por la AEPD en un documento publicado en diciembre de 2018. La Autoridad de Control nacional ofrece, entre otras, las siguientes claves en este sentido:

- **Publicación del Registro de actividades de tratamiento del órgano u organismo del Sector Público**. Los órganos y organismos del Sector Público quedan obligados a publicar en su web el inventario de las actividades de tratamiento de datos personales que realizan, identificando quién trata los datos, con qué finalidad y qué base jurídica legitima ese tratamiento.

- **Obligación de información a los ciudadanos sobre el ejercicio de sus derechos**. Los órganos y organismos del Sector Público quedan obligados a incluir en su página web información clara y precisa destinada a los administrados sobre el ejercicio de los derechos de acceso, rectificación, supresión, derecho a la limitación del tratamiento, así como a la portabilidad y oposición.
- **Potestad de verificación de los datos personales de los ciudadanos**. Los órganos y organismos del Sector Público pueden verificar, sin necesidad de solicitar consentimiento del interesado, la exactitud de los datos personales manifestados por los ciudadanos que obren en poder de los órganos y organismos del Sector Público.
- **Nueva regulación de la aportación de documentación por parte de los ciudadanos: modificación del artículo 28 de la Ley 39/2015.** Ya la ley 30/1992 reconocía a los administrados el derecho a no aportar a los procedimientos administrativos los documentos que obrasen en poder de la Administración, o que hubiesen sido elaborados por ésta. La base jurídica del tratamiento de los datos personales por la Administración era el consentimiento del administrado, que se entendía tácitamente concedido si el interesado no se oponía expresamente.

Tanto el Reglamento General de Protección de Datos como la nueva Ley Orgánica eliminan la necesidad de recabar el consentimiento, ni siquiera tácito, del ciudadano, al establecer como base jurídica legitimadora principal del tratamiento de datos personales por órganos y organismos del Sector Público el cumplimiento de una misión en interés público o, particularmente, el ejercicio de poderes públicos.

Asimismo, la nueva redacción otorgada por la Ley Orgánica al artículo 28 de la Ley 39/2015 reconoce al interesado la posibilidad de oponerse a que órganos y organismos del Sector Público consulten o recaben los citados documentos, pero en ese caso el administrado deberá aportarlos necesariamente para que la Administración pueda conocer que concurren en él los requisitos establecidos por la norma. En caso contrario no podrán estimar su solicitud, precisamente porque no habría demostrado los requisitos requeridos.

En todo caso, dicho derecho de oposición no juega en los casos de potestades de verificación o inspección.

- **Notificación de actos administrativos: identificación de los ciudadanos**. **La nueva Ley impide el uso conjunto apellidos, nombre y número completo del documento de identificación oficial de las personas en aquellos actos administrativos que vayan a ser objeto de publicación o notificación por medio de anuncios.**

A partir de la entrada en vigor de la Ley Orgánica:

✓ Cuando un acto administrativo se deba publicar se identificará a la persona mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias de su documento identificativo oficial.

✓ Cuando se trate de notificaciones por medio de anuncios se identificará a la persona exclusivamente con el número de su documento identificativo.

En ambos casos, cuando la persona carezca de documento identificativo se la identificará sólo mediante su nombre y apellidos.

En relación con esta cuestión, la AEPD, en mayo de 2019, ha publicado unas orientaciones para promover la protección de los datos personales de los ciudadanos cuando las Administraciones Públicas realizan publicaciones de actos administrativos. El documento se publica en coordinación con la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía.

La Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y garantía de los derechos digitales (LOPDGDD) incluye en el apartado 1º de su Disposición Adicional 7ª cómo debe identificarse a los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

El criterio, provisional hasta que los órganos de gobierno y las administraciones públicas competentes aprueben disposiciones para la aplicación del apartado 1º de la Disposición Adicional 7ª de la LOPDGDD, pretende evitar que la adopción de otras fórmulas pueda dar lugar a la publicación de cifras numéricas de los documentos identificativos de las personas en posiciones distintas, posibilitando la recomposición íntegra de dichos documentos. Para ello, se ha seleccionado aleatoriamente un grupo de cuatro cifras numéricas, que deberían ser las mismas en todas las publicaciones.

Puede acceder al contenido del documento con las orientaciones en el siguiente enlace: https://www.aepd.es/media/docs/orientaciones-da7.pdf

- **Comunicación de datos personales de los administrados a sujetos privados**. Los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten:

  ✓ o bien cuando cuenten con el consentimiento de los administrados.

  ✓ o bien, cuando aprecien que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.

- **Designación de un Delegado de Protección de Datos (DPD) y comunicación de la designación a la AEPD**. Los órganos y organismos del Sector Público tienen obligación de designar un Delegado de Protección de Datos que cuente con la debida cualificación, de garantizarle los medios necesarios para el

ejercicio de sus funciones y de notificar la designación a la AEPD para su inclusión en el Registro público de Delegados de Protección de Datos.

El Delegado de Protección de Datos no tiene responsabilidad a título personal, por este mero hecho, por las posibles infracciones en materia de protección de datos cometidas por su organización.

- Intervención del Delegado de Protección de Datos en la resolución de reclamaciones en el Sector Público. El Delegado de Protección de Datos del órgano u organismo del Sector Público debe recibir las reclamaciones que les dirijan los administrados, cuando opten por esta vía antes de plantear una reclamación ante la AEPD, y comunicará la decisión adoptada al administrado en el plazo máximo de dos meses.

Asimismo, el Delegado de Protección de Datos deberá recibir las reclamaciones que la AEPD decida trasladarle con carácter previo al inicio de un expediente sancionador. El Delegado debe comunicar la decisión adoptada al administrado y a la AEPD en el plazo máximo de un mes.

De esta forma, con carácter general, si el Delegado de Protección de Datos consigue que el responsable resuelva por cualquiera de estas dos vías la reclamación, y sin perjuicio de que el interesado posteriormente se dirija a la AEPD, no se iniciaría expediente de declaración de infracción a esa Administración Pública.

- Mayor transparencia de las sanciones impuestas al Sector Público. Las infracciones cometidas por los órganos y organismos del Sector Público serán sancionadas con un apercibimiento con medidas correctoras y no tendrán sanción económica.

La resolución sancionadora de la AEPD identificará el cargo responsable de la infracción, se notificará al infractor, a su superior jerárquico, al Defensor del Pueblo y se publicará en la página web de la AEPD y en el diario oficial correspondiente.

La resolución sancionadora podrá proponer al órgano u organismo la iniciación de actuaciones disciplinarias, cuya resolución deberá ser comunicada por el órgano u organismo del Sector Público a la AEPD.

Las infracciones sean imputables a autoridades y directivos del Sector Público y se acredite la existencia de informes técnicos o recomendaciones que no hubieran sido atendidos por estos, la resolución sancionadora incluirá una amonestación con la identificación del cargo responsable y se publicará en el diario oficial correspondiente.

- Tratamiento de datos personales en la notificación de incidentes de seguridad. Las autoridades públicas, los equipos de respuesta a emergencias informáticas (CERT), los equipos de respuesta a incidentes de seguridad informática (CSIRT), los proveedores de redes y servicios de comunicaciones electrónicas y los proveedores de tecnologías y servicios de seguridad pueden tratar los datos personales contenidos en las notificaciones de incidentes de

seguridad exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta, adoptando siempre las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo.

- Registros de personal del sector público: legitimación del tratamiento. La nueva Ley Orgánica establece que la base legitimadora del tratamiento de datos personales que realizan los registros de personal del sector público es el ejercicio de potestades públicas.

  Estos registros pueden tratar los datos personales que sean estrictamente necesarios para el cumplimiento de sus fines relativos a infracciones y condenas penales e infracciones y sanciones administrativas, de los que deberán ser informados de manera expresa, clara e inequívoca.

- Derechos de los empleados públicos: mayor intimidad. La Ley Orgánica garantiza el derecho a la intimidad de los empleados públicos en el lugar de trabajo frente al uso de dispositivos de video vigilancia y de grabación de sonidos, así como frente al uso de los dispositivos digitales y sistemas de geolocalización.

- Adaptación a la Ley Orgánica de los contratos de encargo de tratamiento de datos personales. Los contratos de encargo de tratamiento de datos personales entre los órganos y organismos del Sector Público (como responsables) y otros órganos u organismos del sector público o terceros (como encargados de tratamiento) suscritos antes del 25 de mayo de 2018 mantendrán su vigencia como máximo hasta el 25 de mayo de 2022.

- Tratamiento de datos personales por concesionarios de servicios públicos. Los órganos y organismos del Sector Público mantendrán el control sobre los datos personales de los usuarios de los servicios públicos aunque haya finalizado la vigencia del contrato de concesión de servicios.

  En el Sector Público, un concesionario de servicios, encargado del tratamiento de datos personales, no se convierte nunca en responsable aunque establezca relaciones con las personas a cuyos datos ha accedido en virtud de la prestación del servicio.

## 3. EL DELEGADO DE PROTECCIÓN DE DATOS Y SUS ESPECIALIDADES EN EL SECTOR PÚBLICO

El RGPD prevé la obligatoriedad de designar un Delegado de Protección de Datos (*DPD*) en determinados supuestos. Se trata de una figura cuyo antecedente puede encontrarse en el artículo 18.2 de la Directiva 95/46/CE, con el nombre de un encargado de protección de datos, cuya designación opcional por el responsable le permitía exceptuar la obligación de notificar los tratamientos a la autoridad nacional de control, dado que sus funciones se centraban en llevar un registro de los tratamientos efectuados por el responsable y en aplicar de manera independiente la normativa de protección de datos en el ámbito interno del responsable.

En el nuevo marco normativo, el DPD es configurado como un colaborador

necesario del responsable o encargado del tratamiento y como un asesor y supervisor del cumplimiento de la normativa de protección de datos, obligatorio en el ámbito de la Administración Pública.

El considerando 97 RGPD establece los ejes de esta nueva figura del DPD:

"Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente."

El RGPD dedica los artículos 37 a 39 a establecer el régimen jurídico del DPD, aunque se encuentran referencias a lo largo del resto del articulado. Esta regulación debe complementarse con la contenida en los artículos 34 a 37 LOPDGDD.

Para una adecuada comprensión de la figura puede acudirse a las "Directrices sobre los delegados de protección de datos (DPD)", adoptadas, por el Grupo de Trabajo del Artículo 29[6], el 13 de diciembre de 2016 y revisadas el 5 de abril de 2017

Sin perjuicio de abordar en la Jornada, de manera más específica, las implicaciones y decisiones que deben adoptarse en el sector público a la hora de designar un DPD, se reseñan en este documento las grandes líneas de esta figura con el fin de procurar el debate posterior entre los participantes.

## 1. Designación

El artículo 37 RGPD se ocupa de la designación del DPD, estableciendo, sin perjuicio de que proceda su nombramiento su obligatoriedad para responsables o encargados de tratamiento siempre que:

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

[6] .- Este grupo de trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE como un órgano consultivo independiente de la UE en materia de protección de datos y privacidad. Sus funciones han sido asumidas en el RGPD por el Comité Europeo de Protección de Datos.

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

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

Nada impide que cualquier organización lo pueda designar voluntariamente o si así lo exige la legislación de un Estado miembro (artículo 37.4 RGPD). Así lo ha hecho España en el artículo 34 LOPDGDD que lo impone, en todo caso, para las siguientes entidades:

a. Los colegios profesionales y sus consejos generales.
b. Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
c. Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
d. Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
e. Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
f. Los establecimientos financieros de crédito.
g. Las entidades aseguradoras y reaseguradoras.
h. Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
i. Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
j. Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
k. Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
l. Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun

estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

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

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

o. Las empresas de seguridad privada.

p. Las federaciones deportivas cuando traten datos de menores de edad.

Esta designación debe comunicarse a las autoridades de control. Los responsables y encargados del tratamiento comunicarán, en cumplimiento de lo dispuesto en el artículo 34 LOPDGDD, en el plazo de diez días a la AEPD o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria. La AEPD y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

Es posible designar un DPD único para varias organizaciones, así resulta del artículo 37.2 RGPD, que permite a un grupo empresarial designar un único DPD, siempre que este «sea fácilmente accesible desde cada establecimiento».

De conformidad con el artículo 37, apartado 3, se podrá designar un único DPD para varias autoridades u organismos públicos, teniendo en cuenta su estructura organizativa y tamaño. Las mismas consideraciones se aplican con respecto a los recursos y las comunicaciones. Puesto que el DPD se encarga de una variedad de tareas, el responsable o el encargado del tratamiento deben garantizar que un único DPD, con la ayuda de un equipo si fuera necesario, pueda realizar dichas tareas eficazmente a pesar de haber sido designado por varias autoridades y organismos públicos.

Como advierte la AEPD (*El nuevo RGPD y su impacto sobre la actividad de las administraciones locales*): "En el ámbito de las AALL las dimensiones de las organizaciones harán inviable en muchos casos que una entidad local cuente con un DPD integrado en su plantilla, ya sea a tiempo completo o a tiempo parcial. Por ello, será preciso encontrar soluciones que permitan que los entes locales cumplan las obligaciones del RGPD en este punto de una forma que se adapte a sus especiales características. Entre las posibles opciones se encuentra la contratación de la actividad de DPD por parte de varias entidades como prestación de servicios o el establecimiento de servicios de DPD a disposición de los municipios en las Diputaciones Provinciales".

Del mismo modo, es posible que el DPD forme parte de la plantilla del responsable o encargado del tratamiento o sea un externo a la organización (artículo 37.6 RGPD), así como que los responsables y encargados del tratamiento establezcan su dedicación completa o a tiempo parcial, entre otros criterios, en función del volumen de

los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados (art. 34.5LOPDGDD).

### 2. Competencias profesionales requeridas

El artículo 37.5 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 indicadas en el artículo 39». En consecuencia, se requiere tener conocimientos especializados sobre la legislación y prácticas nacionales y europeas en materia de protección de datos y una profunda comprensión del RGPD, del sector de la entidad u organización en la que va a desempeñar sus funciones y de tecnologías de la información y de la seguridad de los datos.

El artículo 35 LOPDGDD, dedicado a la cualificación del delegado de protección de datos establece la posibilidad de certificar la formación o preparación para el ejercicio como DPD:

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

En España, la Agencia Española de Protección de Datos aprobó en 2017 un esquema de certificación de DPDs. Aunque esta certificación no es obligatoria para poder ejercer como DPD y se puede ejercer la profesión sin estar certificado bajo éste o cualquier otro esquema, la Agencia ha considerado necesario ofrecer un punto de referencia al mercado sobre los contenidos y elementos de un mecanismo de certificación que pueda servir como garantía para acreditar la cualificación y capacidad profesional de los candidatos a DPD. Toda la información sobre tal esquema está disponible en la web de la AEPD:

https://www.aepd.es/reglamento/cumplimiento/delegado-de-proteccion-de-datos.html

### 3. Funciones

El artículo 39 RGPD establece que el DPD tendrá, como mínimo, las siguientes funciones, que desempeñará 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:

> *a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;*
>
> *b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en*

*materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;*

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

*d) cooperar con la autoridad de control;*

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

El artículo 38.6 RGPD permite, además, que un DPD pueda «desempeñar otras funciones y cometidos». No obstante, requiere que la organización garantice que «dichas funciones y cometidos no den lugar a conflicto de intereses»; un requisito estrechamente ligado a la independencia de que goza en su actuación. Aunque los DPDs puedan tener otras funciones, solamente podrán confiárseles otras tareas y cometidos si estas no dan lugar a conflictos de intereses.

Según el documento de la AEPD sobre "El Delegado de Protección de Datos en las Administraciones Públicas", estas funciones genéricas del DPD se pueden concretar en tareas de asesoramiento y supervisión en, entre otras, las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos
- Identificación de las bases jurídicas de los tratamientos
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia
- Diseño e implantación de políticas de protección de datos

- Auditoría de protección de datos
- Establecimiento y gestión de los registros de actividades de tratamiento
- Análisis de riesgo de los tratamientos realizados
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal en materia de protección de datos

Tales funciones han sido ampliadas en la LOPDGDD, cuyo artículo 37, bajo la rúbrica "Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos", señala:

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

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

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

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

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos."

**4. Posición y estatuto**

La situación del DPD en el seno de una entidad u organización se caracteriza por las siguientes notas:

a. Participación

Se prevé una garantía de su participación en "todas las cuestiones relativas a la protección de datos personales" (artículo 38.1 RGPD).

b. Independencia y rendición de cuentas al más alto nivel

Se garantiza que no recibirá ninguna instrucción en lo que respecta al desempeño de sus funciones, no pudiendo ser destituido ni sancionado por su desempeño, y rindiendo cuentas al más alto nivel jerárquico de la organización (artículo 38.3 RGPD)

c. Confidencialidad

El DPD está obligado a mantener el secreto o confidencialidad por el desempeño de sus funciones. Indica el artículo 38.5 RGPD:

"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".

d. Acceso a datos personales por el DPD

El artículo 36.3 LOPDGDD señala que el DPD, en el ejercicio de sus funciones, tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto,

e. Recursos

El artículo 38.2 RGPD prevé que la organización respalde a su DPD «facilitando los recursos necesarios para el desempeño de [sus] funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados».

f. Protección frente a remociones y sanciones

El artículo 38.3 establece que el DPD «no será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones». La LOPDGDD refuerza este aspecto indicado: "Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses" (art. 36.2).

## 4. REFERENCIAS BIBLIOGRÁFICAS Y DOCUMENTOS DE INTERÉS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). Documentos:

- *El impacto del Reglamento General de Protección de Datos sobre la actividad de las administraciones públicas.*
- *El nuevo RGPD y su impacto sobre la actividad de las administraciones locales*
- *El Delegado de Protección de Datos en las Administraciones Públicas*
- *Orientación para la aplicación provisional de la disposición adicional séptima de la LOPDGDD.*
- *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Nuevas obligaciones para el sector público.*

ALMONACID, VÍCTOR, "El Delegado de Protección de Datos en la Administración Local", accesible en https://nosoloaytos.wordpress.com/2018/03/28/el-delegado-de-proteccion-de-datos-en-laadministracion-local-dpo/#more-13764.

CAMPOS ACUÑA, Concepción "Los 7 imprescindibles en protección de datos para el ámbito local", *El Consultor de los Ayuntamientos y Juzgados*, enero 2018.

DURÁN CARDO, Belén *El Delegado de Protección de Datos en el RGPD y la nueva LOPDGDD*, Wolter Kluwer, 2019.

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre los delegados de protección de datos (DPD)*, adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017, Grupo de Trabajo sobre la protección de Datos del Artículo 29. 16/ES WP 243, rev. 1.

JIMÉNEZ ASENSIO, Rafael "El delegado de protección de datos: perfil y encuadre en las organizaciones públicas (en especial en los entes locales), 22.03.2018, accesible en http://laadministracionaldia.inap.es/noticia.asp?id=1508368.

SIMÓN CASTELLANO, PERE, *El desempeño de las funciones de Delegado de Protección de Datos*, Bosch, 2018.