GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

16/ES
WP 243 rev.01

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

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

Vistos los artículos 29 y 30 de dicha Directiva,

Visto su Reglamento interno,

HA ADOPTADO LAS PRESENTES DIRECTRICES:

Índice

TOC

1 Introducción

El Reglamento general sobre protección de datos (RGPD),[1] cuya entrada en vigor está prevista el 25 de mayo de 2018, proporciona un marco modernizado y basado en la rendición de cuentas para la protección de los datos en Europa. Los delegados de protección de datos (DPD) serán el elemento central de este nuevo marco jurídico para muchas organizaciones, facilitando el cumplimiento de las disposiciones del RGPD.

En virtud del RGPD, es obligatorio que algunos responsables y encargados del tratamiento designen un DPD.[2] Así será en el caso de todas las autoridades y organismos públicos (con independencia de qué datos traten), y de otras organizaciones cuya actividad fundamental consista en la observación sistemática de personas a gran escala, o que traten categorías especiales de datos personales a gran escala.

Incluso en algunos casos en los que el RGPD no requiera específicamente el nombramiento de un DPD, las organizaciones pueden considerar de utilidad designar un DPD de manera voluntaria. El Grupo de Trabajo sobre protección de datos del artículo 29 alienta estos esfuerzos voluntarios.

El concepto de DPD no es nuevo. Aunque la Directiva 95/46/CE[3] no exigía a ninguna organización el nombramiento de un DPD, la práctica de tal designación se ha desarrollado, no obstante, en varios Estados miembros a lo largo de los años.

Antes de la adopción del RGPD, el Grupo de Trabajo del artículo 29 argumentaba que el DPD es la piedra angular de la rendición de cuentas y que el nombramiento de un DPD puede facilitar el cumplimiento y, además, convertirse en una ventaja competitiva para las empresas.[4] Además de facilitar el cumplimiento mediante la aplicación de instrumentos de rendición de cuentas (tales como facilitar o llevar a cabo evaluaciones de impacto y auditorías de protección de datos), los DPD actúan como intermediarios entre las partes interesadas correspondientes (p. ej. autoridades de control, interesados y unidades de negocio dentro de una organización).

---

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (DO L 119 de 4.5.2016). El RGPD es pertinente a efectos del EEE y se aplicará tras su incorporación al Acuerdo EEE.

[2] El nombramiento de un DPD es también obligatorio para las autoridades competentes en virtud del artículo 32 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89), y la legislación nacional de aplicación. Aunque las presentes directrices se centran en los DPD en virtud del RGPD, la orientación es también pertinente con respecto a los DPD con arreglo a la Directiva 2016/680, en lo referente a sus disposiciones similares.

[3] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

[4] Véase http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

Los DPD no son personalmente responsables en caso de incumplimiento del RGPD. El RGPD deja claro que es el responsable o el encargado del tratamiento quien está obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza de conformidad con sus disposiciones (artículo 24, apartado 1). El cumplimiento de las normas sobre protección de datos es responsabilidad del responsable o del encargado del tratamiento.

Asimismo, el responsable o el encargado del tratamiento tiene un papel fundamental a la hora de posibilitar el desempeño efectivo de las tareas del DPD. El nombramiento de un DPD es un primer paso, pero el DPD debe contar además con la autonomía y los recursos suficientes para desarrollar su labor de forma efectiva.

El RGPD reconoce al DPD como participante clave en el nuevo sistema de gestión de los datos y establece las condiciones para su nombramiento, su puesto y sus tareas. El objetivo de estas directrices es aclarar las disposiciones pertinentes del RGPD con el fin de ayudar a los responsables y encargados del tratamiento a cumplir con la legislación, pero también ayudar a los DPD en el desempeño de su labor. Las directrices ofrecen, además, recomendaciones sobre las mejores prácticas, basadas en la experiencia adquirida en algunos Estados miembros de la UE. El Grupo de Trabajo del artículo 29 supervisará la aplicación de las presentes directrices y podrá complementarlas con datos adicionales cuando proceda.

2 Designación de un DPD

2.1. Designación obligatoria

El artículo 37, apartado 1, del RGPD requiere la designación de un DPD en tres casos específicos:[5]

a) cuando el tratamiento lo lleve a cabo una autoridad u organismo público;[6]
b) cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance o fines, requieran una observación habitual y sistemática de interesados a gran escala; o
c) cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales[7] o[8] de datos relativos a condenas e infracciones penales[9].

En las siguientes subsecciones, el Grupo de Trabajo del artículo 29 ofrece orientación sobre los criterios y la terminología utilizados en el artículo 37, apartado 1.

[5] Téngase en cuenta que, con arreglo al artículo 37, apartado 4, el Derecho de la Unión o de los Estados miembros podrá exigir el nombramiento de un DPD también en otras situaciones.

[6] Excepto los tribunales que actúen en el ejercicio de su función judicial. Véase el artículo 32 de la Directiva (UE) 2016/680.

[7] De conformidad con el artículo 9, esto incluye datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

[8] El artículo 37, apartado 1, letra c), utiliza la palabra «*y*». Véase en la sección 2.1.5 a continuación la explicación del uso de «*o*» en lugar de «*y*».

[9] Artículo 10.

A menos que resulte obvio que a una organización no se le requiere la designación de un DPD, el Grupo de Trabajo del artículo 29 recomienda que los responsables y encargados del tratamiento documenten el análisis interno realizado para determinar si debe nombrarse o no un DPD, a fin de poder demostrar que se han tenido en cuenta debidamente los factores pertinentes[10]. Este análisis forma parte de la documentación requerida con arreglo al principio de rendición de cuentas. Puede ser exigido por la autoridad de control y debe actualizarse cuando sea necesario, por ejemplo, si los responsables o los encargados del tratamiento llevan a cabo nuevas actividades o prestan servicios nuevos que puedan incluirse en los casos enumerados en el artículo 37, apartado 1.

Cuando una organización designe un DPD de forma voluntaria, se aplicarán a su designación, su puesto y sus tareas los requisitos establecidos en los artículos 37 a 39, como si el nombramiento hubiera sido obligatorio.

Nada impide a una organización que legalmente no está obligada a designar un DPD y no desea nombrarlo de forma voluntaria emplear a pesar de todo personal o asesores externos que desempeñen tareas relacionadas con la protección de los datos personales. En ese caso, es importante asegurarse de que no haya confusión posible con respecto a su cargo, estatus, puesto y tareas. Por ello, debe quedar claro, en cualquier comunicación dentro de la empresa, así como con las autoridades de protección de datos, los interesados y el público en general, que el título de esta persona o asesor no es el de delegado de protección de datos (DPD). [11]

El DPD, ya sea obligatorio o voluntario, se designa para todas las operaciones de tratamiento llevadas a cabo por el responsable o el encargado del tratamiento.

[10] Véase el artículo 24, apartado 1.

[11] Esto es también pertinente para los responsables de la protección de la intimidad u otros profesionales encargados de la protección de la intimidad que ya existen en algunas empresas, los cuales puede que no siempre satisfagan los criterios del RGPD, por ejemplo en cuanto a recursos disponibles o garantías de independencia, y por consiguiente no pueden considerarse DPD ni hacerse mención a ellos como tales.

2.1.1 «AUTORIDAD U ORGANISMO PÚBLICO»

El RGPD no define qué constituye una «autoridad u organismo público». El Grupo de Trabajo del artículo 29 considera que dicha noción debe determinarse en virtud del Derecho nacional. Por consiguiente, las autoridades y organismos públicos incluyen las autoridades nacionales, regionales y locales, pero además el concepto, con arreglo a la legislación nacional aplicable, normalmente incluye también una serie de organismos regidos por el derecho público.[12] En tales casos, la designación de un DPD es obligatoria.

Una labor pública puede llevarse a cabo, y la autoridad pública puede ejercerse[13], no solo por las autoridades y organismos públicos sino también por otras personas físicas o jurídicas regidas por el derecho público o privado, en sectores como, según la legislación nacional de cada Estado miembro, los servicios de transporte público, el suministro de agua y energía, las infraestructuras viarias, la radiodifusión pública, la vivienda pública o los órganos disciplinarios de las profesiones reguladas.

En estos casos, los interesados pueden estar en una situación muy similar a la que se produce cuando una autoridad u organismo público trata sus datos. En particular, los datos pueden tratarse para fines similares y las personas suelen tener un poder de decisión igualmente escaso o nulo sobre si sus datos se tratan y de qué manera, y pueden, por tanto, requerir la protección adicional que pueda aportar la designación de un DPD.

Aunque no existe obligación en tales casos, el Grupo de Trabajo del artículo 29 recomienda como buena práctica que las organizaciones privadas que llevan a cabo una función pública o ejercen autoridad pública designen un DPD. La actividad de dicho DPD abarca todas las operaciones de tratamiento realizadas, también las que no están relacionadas con el desempeño de una función pública o el ejercicio de una autoridad pública (p. ej. la gestión de una base de datos de empleados).

2.1.2 «ACTIVIDADES PRINCIPALES»

El artículo 37, apartado 1, letras b) y c), del RGPD se refiere a las «actividades principales del responsable o del encargado». El considerando 97 especifica que 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». Las «actividades principales» pueden considerarse las operaciones clave necesarias para lograr los objetivos del responsable o del encargado del tratamiento.

No obstante, las «actividades principales» no deben interpretarse como excluyentes cuando el tratamiento de datos sea una parte indisociable de la actividad del responsable o encargado del tratamiento. Por ejemplo, la actividad principal de un hospital es prestar atención sanitaria. Sin embargo, un hospital no podría prestar atención sanitaria de manera segura y eficaz sin tratar datos relativos a la salud, como las historias clínicas de los pacientes. Por tanto, el tratamiento de dichos

[12] Véase, p. ej. la definición de «organismo del sector público» y de «organismo de Derecho público» en el artículo 2, números 1 y 2, de la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público (DO L 345 de 31.12.2003, p.90).

[13] Artículo 6, apartado 1, letra e).

datos debe considerarse una de las actividades principales de cualquier hospital y los hospitales deben, en consecuencia, designar un DPD.

Otro ejemplo sería el de una empresa de seguridad privada que lleva a cabo la vigilancia de una serie de centros comerciales privados y de espacios públicos. La vigilancia es la actividad principal de la empresa, que a su vez está ligada de manera indisociable al tratamiento de datos personales. Por tanto, esta empresa debe también designar un DPD.

Por otra parte, todas las organizaciones llevan a cabo determinadas actividades, por ejemplo, pagar a sus empleados o realizar actividades ordinarias de apoyo de TI. Dichas actividades son ejemplo de funciones de apoyo necesarias para la actividad principal o el negocio principal de la organización. Aunque estas actividades son necesarias o esenciales, normalmente se consideran funciones auxiliares y no la actividad principal.

2.1.3 «A GRAN ESCALA»

El artículo 37, apartado 1, letras b) y c), dispone que el tratamiento de datos personales debe realizarse a gran escala para provocar la designación de un DPD. El RGPD no define qué se entiende por tratamiento a gran escala, aunque el considerando 91 ofrece alguna orientación.[14]

De hecho, no es posible dar una cifra exacta, ya sea con relación a la cantidad de datos procesados o al número de personas afectadas, que pudiera aplicarse en todas las situaciones. No obstante, esto no excluye la posibilidad de que, con el tiempo, se desarrolle un método estándar para identificar en términos más específicos o cuantitativos qué constituye «a gran escala» con respecto a determinados tipos de actividades de tratamiento comunes. El Grupo de Trabajo del artículo 29 también prevé contribuir a este desarrollo compartiendo y publicando ejemplos de los umbrales pertinentes para la designación de un DPD.

En cualquier caso, el Grupo de Trabajo recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala:

- el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
- el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento;
- la duración, o permanencia, de la actividad de tratamiento de datos;
- el alcance geográfico de la actividad de tratamiento.

[14] Según el considerando, se incluirían en particular «las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo». Por otra parte, el considerando dispone específicamente que «el tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud o abogado». Es importante tener en cuenta que, aunque el considerando proporciona ejemplos situados en los extremos de la escala (tratamiento de datos de un solo médico frente al tratamiento de datos en la totalidad de un país o en toda Europa), hay una amplia zona gris entre ambos extremos. Además, debe tenerse en cuenta que este considerando se refiere a las evaluaciones de impacto relativas a la protección de datos. Esto significa que algunos elementos pueden ser específicos de dicho contexto y no aplicarse necesariamente de la misma manera a la designación de los DPD.

Como ejemplos de tratamiento a gran escala cabe citar:

- el tratamiento de datos de pacientes en el desarrollo normal de la actividad de un hospital;
- el tratamiento de datos de desplazamiento de las personas que utilizan el sistema de transporte público de una ciudad (p. ej. seguimiento a través de tarjetas de transporte);
- el tratamiento de datos de geolocalización en tiempo real de clientes de una cadena internacional de comida rápida con fines estadísticos por parte de un responsable del tratamiento especializado en la prestación de estos servicios;
- el tratamiento de datos de clientes en el desarrollo normal de la actividad de una compañía de seguros o de un banco;
- el tratamiento de datos personales para publicidad comportamental por un motor de búsqueda;
- el tratamiento de datos (contenido, tráfico, ubicación) por proveedores de servicios de telefonía o internet.

Como casos que no constituyen tratamiento a gran escala cabe señalar:

- el tratamiento de datos de pacientes por parte de un solo médico;
- el tratamiento de datos personales relativos a condenas e infracciones penales por parte de un abogado.

2.1.4 «OBSERVACIÓN HABITUAL Y SISTEMÁTICA»

La noción de observación habitual y sistemática de interesados no está definida en el RGPD, pero el concepto de «observación del comportamiento de los interesados» se menciona en el considerando 24[15] e incluye claramente toda forma de seguimiento y creación de perfiles en internet, también con fines de publicidad comportamental.

No obstante, el concepto de observación no se limita al entorno en línea y el seguimiento en línea debe considerarse solo un ejemplo de observación del comportamiento de los interesados[16].

El Grupo de Trabajo del artículo 29 interpreta «habitual» con uno o más de los siguientes significados:

- continuado o que se produce a intervalos concretos durante un periodo concreto;
- recurrente o repetido en momentos prefijados;
- que tiene lugar de manera constante o periódica.

El Grupo de Trabajo interpreta «sistemático» con uno o más de los siguientes significados:

- que se produce de acuerdo con un sistema;
- preestablecido, organizado o metódico;

[15] *«Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes».*

[16] Téngase en cuenta que el considerando 24 se centra en la aplicación extraterritorial del RGPD. Además, existe también una diferencia textual entre «control de su comportamiento» [artículo 3, apartado 2, letra b)] y «observación habitual y sistemática de los interesados» [artículo 37, apartado 1, letra b)] que podría, por tanto, considerarse una noción distinta.

- que tiene lugar como parte de un plan general de recogida de datos;
- llevado a cabo como parte de una estrategia.

Ejemplos de actividades que pueden constituir una observación habitual y sistemática de interesados son: operar una red de telecomunicaciones; prestar servicios de telecomunicaciones; redireccionar correos electrónicos; actividades de mercadotecnia basadas en datos; elaborar de perfiles y otorgar puntuación con fines de evaluación de riesgos (p. ej. para determinar la calificación crediticia, establecer primas de seguros, prevenir el fraude, detectar blanqueo de dinero); llevar a cabo un seguimiento de la ubicación, por ejemplo, mediante aplicaciones móviles; programas de fidelidad; publicidad comportamental; seguimiento de los datos de bienestar, estado físico y salud mediante dispositivos ponibles; televisión de circuito cerrado; dispositivos conectados, como contadores inteligentes, coches inteligentes, domótica, etc.

2.1.5 CATEGORÍAS ESPECIALES DE DATOS Y DATOS RELATIVOS A CONDENAS E INFRACCIONES PENALES

El artículo 37, apartado 1, letra c), aborda el tratamiento de las categorías especiales de datos con arreglo al artículo 9 y los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10. Aunque la disposición emplea la palabra «y», no existe ningún motivo normativo que obligue a aplicar ambos criterios simultáneamente, y, por tanto, debe leerse el texto como si dijera «o».

2.2. Delegado de protección de datos del encargado del tratamiento

El artículo 37 se aplica tanto a los responsables del tratamiento[17] como a los encargados del tratamiento[18] con respecto a la designación de un DPD. En función de quién cumpla los criterios de designación obligatoria, en algunos casos solo el responsable o solo el encargado deben designar un DPD, y en otros casos tanto el responsable como su encargado deben designar respectivos DPD (que deberán cooperar entre sí).

Es importante destacar que, aunque el responsable cumpla los criterios de designación obligatoria, su encargado no está necesariamente obligado a nombrar un DPD. No obstante, puede ser una práctica recomendable.

Ejemplos:

- Una pequeña empresa familiar que se dedica a la distribución de electrodomésticos en una única ciudad utiliza los servicios de un responsable del tratamiento cuya actividad principal es prestar servicios de análisis web y asistencia en materia de publicidad dirigida y mercadotecnia. Las actividades de la empresa familiar y sus clientes no generan un tratamiento de datos «a gran escala», teniendo en cuenta el reducido número de clientes y las actividades relativamente limitadas. No obstante, las actividades del responsable del

[17] El responsable del tratamiento se define en el artículo 4, punto 7, como la persona u organismo que determine los fines y medios del tratamiento.

[18] El encargado del tratamiento se define en el artículo 4, punto 8, como la persona u organismo que trate datos por cuenta del responsable.

tratamiento, que tiene muchos clientes como esta pequeña empresa, tomadas en su conjunto, constituyen un tratamiento a gran escala. El responsable del tratamiento deberá, por tanto, designar un DPD, de conformidad con el artículo 37, apartado 1, letra b). Al mismo tiempo, la empresa familiar no está sujeta a la obligación de designar un DPD.

- Una empresa mediana que fabrica azulejos subcontrata sus servicios de salud laboral a un responsable del tratamiento externo con un gran número de clientes similares. El responsable del tratamiento designará un DPD en virtud del artículo 37, apartado 1, letra c), siempre que el tratamiento se realice a gran escala. No obstante, el fabricante no estará necesariamente obligado a designar un DPD.

El DPD designado por un encargado del tratamiento también supervisará las actividades realizadas por la organización del encargado cuando actúe como responsable del tratamiento por derecho propio (p. ej. RR HH, TI, logística).

2.3. Designación de un DPD único para varias organizaciones

El artículo 37, apartado 2, permite a un grupo empresarial designar un único DPD, siempre que este «sea fácilmente accesible desde cada establecimiento». La noción de accesibilidad se refiere a las tareas del DPD como punto de contacto con respecto a los interesados[19] y a la autoridad de control[20], pero también internamente dentro de la organización, teniendo en cuenta que una de esas tareas es «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».[21]

Con el fin de garantizar que el DPD, ya sea interno o externo, sea accesible, es importante asegurarse de que sus datos de contacto están disponibles de conformidad con los requisitos del RGPD.[22]

El DPD, con ayuda de un equipo si es necesario, debe estar en condiciones de comunicarse eficazmente con los interesados[23] y cooperar[24] con las correspondientes autoridades de control. Esto significa también que dicha comunicación debe tener lugar en el idioma o idiomas utilizados por las autoridades de control y los interesados afectados. La disponibilidad de un DPD (ya sea físicamente en las mismas instalaciones como empleado, ya sea en línea o mediante otros medios seguros de comunicación) es fundamental para garantizar que los interesados puedan contactar con el DPD.

[19] Artículo 38, apartado 4: «*Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento*».

[20] Artículo 39, apartado 1, letra 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*».

[21] Artículo 39, apartado 1, letra a).

[22] Véase también la siguiente sección 2.6.

[23] Artículo 12, apartado 1: *«El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño».*

[24] Artículo 39, apartado 1, letra d): *«cooperar con la autoridad de control».*

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.

2.4. Accesibilidad y ubicación del DPD

De conformidad con la sección 4 del RGPD, la accesibilidad del DPD debe ser efectiva.

Para garantizar que el DPD sea accesible, el Grupo de Trabajo del artículo 29 recomienda que el DPD se encuentre en la Unión Europea, con independencia de si el responsable o el encargado del tratamiento está establecido en ella.

No obstante, no debe excluirse que, en algunas situaciones en las que el responsable o el encargado del tratamiento no tenga establecimiento en la Unión Europea[25], un DPD pueda llevar a cabo sus actividades de manera más eficaz si se encuentra situado fuera de la Unión Europea.

2.5. Conocimientos y habilidades del DPD

El artículo 37, apartado 5, establece que el delegado de protección de datos «será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39». El considerando 97 dispone que el nivel de conocimientos especializados necesario se debe determinar en función de las operaciones de tratamiento de datos que se realicen y de la protección exigida para los datos personales tratados.

- **Nivel de conocimientos**

El nivel de conocimientos requerido no está definido estrictamente pero debe ser acorde con la sensibilidad, complejidad y cantidad de los datos que una organización trata. Por ejemplo, cuando la actividad de tratamiento de los datos es especialmente compleja o cuando implica una gran cantidad de datos sensibles, el DPD podría necesitar un nivel mayor de conocimientos y apoyo. Existe también una diferencia dependiendo de si la organización transfiere sistemáticamente datos personales fuera de la Unión Europea o si dichas transferencias son ocasionales. Así pues, el DPD debe elegirse con cuidado, teniendo debidamente en cuenta las cuestiones relativas a la protección de datos que surjan en la organización.

- **Cualidades profesionales**

Aunque el artículo 37, apartado 5, no especifica las cualidades profesionales que se deben tener en cuenta a la hora de designar al DPD, un factor importante es que este tenga conocimientos sobre la legislación y prácticas nacionales y europeas en materia de protección de datos y una profunda

[25] Véase el artículo 3 del RGPD relativo al ámbito territorial.

comprensión del RGPD. Resulta también de utilidad que las autoridades de control promuevan una formación adecuada y periódica para los DPD.

El conocimiento del sector empresarial y de la organización del responsable del tratamiento es también útil. Asimismo, el DPD debe tener un buen conocimiento de las operaciones de tratamiento que se llevan a cabo, así como de los sistemas de información y de las necesidades de seguridad y protección de datos del responsable del tratamiento.

En el caso de una autoridad u organismo público, el DPD debe también poseer un conocimiento sólido de las normas y procedimientos administrativos de la organización.

- **Capacidad para desempeñar sus funciones**

La capacidad del DPD para desempeñar sus funciones debe interpretarse tanto en referencia a sus cualidades personales y conocimientos como a su puesto dentro de la organización. Las cualidades personales deben incluir, por ejemplo, la integridad y un nivel elevado de ética profesional; la principal preocupación del DPD debe ser posibilitar el cumplimiento del RGPD. El DPD desempeña un papel fundamental en la promoción de una cultura de protección de datos dentro de la organización y contribuye a la aplicación de elementos esenciales del RGPD, como los principios relativos al tratamiento de datos[26], los derechos de los interesados[27], la protección de los datos desde el diseño y por defecto[28], el registro de las actividades de tratamiento[29], la seguridad del tratamiento[30] y la notificación y comunicación de las violaciones de la seguridad de los datos.[31]

- **El DPD en el marco de un contrato de servicios**

La función del DPD puede ejercerse también en el marco de un contrato de servicios suscrito con una persona física o con una organización ajena a la organización del responsable o del encargado del tratamiento. En este último caso, es fundamental que cada miembro de la organización que ejerza las funciones de DPD cumpla todos los requisitos aplicables de la sección 4 del RGPD (p.ej. es fundamental que nadie tenga un conflicto de intereses). Es igualmente importante que cada uno de estos miembros esté protegido por las disposiciones del RGPD (p. ej. las que impiden la rescisión injustificada del contrato de servicios motivada por las actividades del DPD, así como la destitución improcedente del miembro de la organización que realice las funciones del DPD). Al mismo tiempo, es posible combinar capacidades y puntos fuertes individuales para que varios individuos que trabajen en equipo puedan servir a sus clientes de forma más eficaz.

En aras de la claridad jurídica y de la buena organización y con el fin de evitar conflictos de intereses de los miembros del equipo, se recomienda asignar claramente las tareas dentro del equipo del DPD y designar una única persona como contacto y persona «a cargo» de cada cliente. Sería también útil, en general, especificar estos puntos en el contrato de servicios.

2.6. Publicación y comunicación de los datos de contacto del DPD

[26] Capítulo II.
[27] Capítulo III.
[28] Artículo 25.
[29] Artículo 30.
[30] Artículo 32.
[31] Artículos 33 y 34.

El artículo 37, apartado 7, del RGPD requiere que el responsable o el encargado del tratamiento:

- publiquen los datos de contacto del DPD y
- comuniquen los datos de contacto del DPD a las correspondientes autoridades de control.

El objetivo de dichos requisitos es garantizar que los interesados (tanto dentro como fuera de la organización) y las autoridades de control puedan contactar de forma fácil y directa con el DPD, sin tener que contactar con ninguna otra parte de la organización. La confidencialidad es igualmente importante: por ejemplo, los empleados pueden ser reacios a presentar quejas al DPD si la confidencialidad de sus comunicaciones no está garantizada.
El DPD 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 (artículo 38, apartado 5).

Los datos de contacto del DPD deben incluir información que permita a los interesados y a las autoridades de control comunicarse con este de forma sencilla (dirección postal, un número de teléfono específico y/o una dirección de correo electrónico específica). Cuando corresponda, a efectos de comunicación con el público, podrían facilitase otros medios de comunicación, por ejemplo, una línea directa específica o un formulario de contacto específico dirigido al DPD en el sitio web de la organización.

El artículo 37, apartado 7, no requiere que los datos de contacto publicados incluyan el nombre del DPD. Aunque hacerlo podría ser una práctica recomendable, corresponde al responsable o al encargado del tratamiento y al DPD decidir si es necesario o útil en cada circunstancia concreta[32].

No obstante, la comunicación del nombre del DPD a la autoridad de control es fundamental, con el fin de que el DPD actúe como punto de contacto entre la organización y la autoridad de control [artículo 39, apartado 1, letra e)].

Como una buena práctica, el Grupo de Trabajo del artículo 29 recomienda también que las organizaciones informen a sus empleados del nombre y datos de contacto del DPD. Por ejemplo, el nombre y los datos de contacto del DPD podrían publicarse internamente en la intranet de la organización, en el directorio telefónico interno y en el organigrama.

[32] Cabe señalar que el artículo 33, apartado 3, letra b), que describe la información que debe facilitarse a la autoridad de control y a los interesados en caso de una violación de la seguridad de los datos personales, requiere específicamente, al contrario que el artículo 37, apartado 7, que se comunique el nombre (y no solo los datos personales) del DPD.

3 Posición del DPD

3.1. Participación del DPD en todas las cuestiones relativas a la protección de datos personales

El artículo 38 del RGPD establece que el responsable y el encargado del tratamiento garantizarán que el DPD «participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales».

Es fundamental que el DPD, o su equipo, participen desde la etapa más temprana posible en todas las cuestiones relativas a la protección de los datos. En cuanto a las evaluaciones de impacto relativas a la protección de datos, el RGPD dispone expresamente la implicación temprana del DPD y especifica que el responsable del tratamiento recabará el asesoramiento del DPD al realizar dicha evaluación de impacto[33]. Garantizar que se informa y consulta al DPD desde el principio facilitará el cumplimiento del RGPD, fomentará un enfoque de privacidad desde el diseño y, por lo tanto, debería ser un procedimiento estándar en la gobernanza de la organización. Asimismo, es importante que el DPD sea considerado como un interlocutor dentro de la organización y que forme parte de los correspondientes grupos de trabajo que se ocupan de las actividades de tratamiento de datos dentro de la organización.

En consecuencia, la organización debe garantizar, por ejemplo, que:

- Se invita al DPD a participar con regularidad en reuniones con los cuadros directivos altos y medios.
- Se recomienda que esté presente cuando se toman decisiones con implicaciones para la protección de datos. Toda la información pertinente debe transmitirse al DPD a su debido tiempo con el fin de que pueda prestar un asesoramiento adecuado.
- La opinión del DPD se tiene siempre debidamente en cuenta. En caso de desacuerdo, el Grupo de Trabajo recomienda, como buena práctica, documentar los motivos por los que no se sigue el consejo del DPD.
- Se consulta al DPD con prontitud una vez que se haya producido una violación de la seguridad de los datos o cualquier otro incidente.

Cuando sea pertinente, el responsable o el encargado del tratamiento podría elaborar directrices o programas sobre la protección de datos que determinen cuándo debe consultarse al DPD.

3.2. Recursos necesarios

El artículo 38, apartado 2, del 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». Deben tenerse en cuenta, en especial, los siguientes aspectos:

- Apoyo activo a la labor del DPD por parte de la alta dirección (al nivel del consejo de administración).
- Tiempo suficiente para que el DPD cumpla con sus funciones, lo cual es particularmente importante cuando se designa un DPD interno a tiempo parcial o cuando el DPD externo lleva

[33] Artículo 35, apartado 2.

a cabo la protección de datos de manera complementaria a otras obligaciones. De otro modo, el conflicto entre prioridades podría dar lugar al descuido de las obligaciones del DPD. Es primordial contar con tiempo suficiente para dedicárselo a las tareas de DPD. Es una práctica recomendable establecer un porcentaje de tiempo para la labor propia del DPD cuando no se lleve a cabo a tiempo completo. Es también práctica recomendable determinar el tiempo necesario para realizar la labor, el nivel de prioridad adecuado para las funciones del DPD y para que el DPD (o la organización) redacte un plan de trabajo.

- Apoyo adecuado en cuanto a recursos financieros, infraestructura (locales, instalaciones, equipos) y personal, según se requiera.
- Comunicación oficial de la designación del DPD a todo el personal para garantizar que su existencia y función se conozcan dentro de la organización.
- Acceso necesario a otros servicios, como recursos humanos, departamento jurídico, TI, seguridad, etc., de modo que los DPD puedan recibir apoyo esencial, aportaciones e información de dichos servicios.
- Formación continua. Debe darse a los DPD la oportunidad de mantenerse al día con respecto a los avances que se den en el ámbito de la protección de datos. El objetivo debe ser mejorar constantemente el nivel de conocimientos de los DPD y se les debe animar a participar en cursos de formación sobre protección de datos y otras formas de desarrollo profesional, como la participación en foros privados, talleres, etc.
- En función del tamaño y estructura de la organización, puede ser necesario establecer un equipo de DPD (un DPD y su personal). En esos casos, deben delimitarse con claridad la estructura interna del equipo y las tareas y responsabilidades de cada uno de sus miembros. De manera similar, cuando la función del DPD la ejerza un proveedor de servicios externo, un grupo de personas que trabaje para dicha entidad podrá realizar de manera eficaz las funciones de DPD como equipo, bajo la responsabilidad de un contacto principal designado para el cliente.

En general, cuanto más complejas o sensibles sean las operaciones de tratamiento, más recursos deberán destinarse al DPD. La función de protección de datos debe desempeñarse con eficacia y dotarse con los recursos suficientes para el tratamiento que se esté realizando.

3.3. Instrucciones y desempeño de «sus funciones y cometidos de manera independiente»

El artículo 38, apartado 3, establece algunas garantías básicas que contribuyen a asegurar que los DPD puedan realizar sus tareas con el suficiente grado de autonomía dentro de su organización. En particular, los responsables o encargados del tratamiento están obligados a garantizar que el DPD «no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones». El considerando 97 añade que los DPD «sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente».

Esto significa que, en el desempeño de sus tareas con arreglo al artículo 39, no debe instruirse a los DPD sobre cómo abordar un asunto, por ejemplo qué resultado debería lograrse, cómo investigar una queja o si se debe consultar a la autoridad de control. Asimismo, no se les debe instruir para que adopten una determinada postura con respecto a un asunto relacionado con la ley de protección de datos, por ejemplo, una interpretación concreta de la ley.

No obstante, la autonomía de los DPD no significa que tengan poder para adoptar decisiones más allá de sus funciones, definidas con arreglo al artículo 39.

El responsable o el encargado del tratamiento sigue siendo responsable del cumplimiento de la normativa de protección de datos y debe ser capaz de demostrar dicho cumplimiento[34]. Si el responsable o el encargado del tratamiento toma decisiones que son incompatibles con el RGPD y el consejo del DPD, este debe tener la posibilidad de expresar con claridad sus discrepancias al más alto nivel de dirección y a los encargados de la toma de decisiones. A este respecto, el artículo 38, apartado 3, establece que el DPD «rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado». Dicha notificación directa garantiza que la alta dirección (p. ej. el consejo de administración) está informada del consejo y recomendaciones del DPD, como parte de la misión del DPD de informar y asesorar al responsable o al encargado del tratamiento. Otro ejemplo de notificación directa es la elaboración de un informe anual de las actividades del DPD que se presentará al más alto nivel directivo.

3.4. Destitución o sanción por el desempeño de las funciones del DPD

El artículo 38, apartado 3, establece que el DPD «no será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones».

Este requisito refuerza la autonomía de los DPD y contribuye a garantizar que actúan de manera independiente y gozan de la suficiente protección en el desempeño de sus funciones de protección de datos.

El RGPD prohíbe las sanciones únicamente si se imponen como resultado del desempeño de las funciones del DPD en cuanto tal. Por ejemplo, es posible que un DPD considere que un tratamiento concreto es susceptible de causar un riesgo elevado y aconseje al responsable o al encargado del tratamiento que realice una evaluación de impacto relativa a la protección de datos, pero que el responsable o el encargado del tratamiento no esté de acuerdo con la valoración del DPD. En un caso así, no puede destituirse al DPD por dar ese consejo.

Las sanciones pueden adoptar formas diversas y pueden ser directas o indirectas. Podrían consistir, por ejemplo, en la falta de ascensos o su dilación, en el impedimento de la promoción profesional o en la denegación de prestaciones que otros empleados reciben. No es necesario que dichas sanciones se impongan realmente, una simple amenaza es suficiente siempre que se utilice para penalizar al DPD por motivos relacionados con el desarrollo de sus actividades.

Como norma general de gestión y como sería el caso para cualquier otro empleado o contratista sujeto al derecho contractual, laboral y penal aplicable en cada país, un DPD podría ser destituido legítimamente por motivos distintos del desempeño de sus funciones como DPD (por ejemplo, en caso de robo, acoso físico, psicológico o sexual o falta grave similar).

En este contexto, cabe señalar que el RGPD no especifica cómo o cuándo puede un DPD ser destituido o sustituido por otra persona. No obstante, cuanto más estable sea el contrato del DPD y más garantías existan contra el despido improcedente, más probabilidad habrá de que el DPD pueda actuar con

[34] Artículo 5, apartado 2.

independencia. Por tanto, el Grupo de Trabajo del artículo 29 acogería con satisfacción los esfuerzos de las organizaciones en este sentido.

3.5. Conflicto de intereses

El artículo 38, apartado 6, permite a los DPD «desempeñar otras funciones y cometidos». No obstante, requiere que la organización garantice que «dichas funciones y cometidos no den lugar a conflicto de intereses».

La ausencia de conflicto de intereses está estrechamente ligada al requisito de actuar de manera independiente. Aunque los DPD puedan tener otras funciones, solamente podrán confiárseles otras tareas y cometidos si estas no dan lugar a conflictos de intereses. Esto supone, en especial, que el DPD no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso.

Como norma general, los cargos en conflicto dentro de una organización pueden incluir los puestos de alta dirección (tales como director general, director de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI) pero también otros cargos inferiores en la estructura organizativa si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento. Asimismo, también puede surgir un conflicto de intereses, por ejemplo, si se pide a un DPD que represente al responsable o al encargado del tratamiento ante los tribunales en casos relacionados con la protección de datos.

Dependiendo de las actividades, tamaño y estructura de la organización, puede ser una práctica recomendable que los responsables y encargados del tratamiento:

- determinen los puestos que podrían ser incompatibles con la función de DPD;
- elaboren normas internas a tal efecto con el fin de evitar conflictos de intereses;
- incluyan una explicación más general sobre los conflictos de intereses;
- declaren que su DPD no tiene ningún conflicto de intereses con respecto a sus funciones como DPD, como medio de concienciar sobre este requisito;
- incluyan salvaguardias en las normas internas de la organización y garanticen que el anuncio de convocatoria para el puesto de DPD o el contrato de servicios sea lo suficientemente preciso y detallado para evitar un conflicto de intereses. En este contexto, debe tenerse en cuenta también que los conflictos de intereses pueden adoptar diversas formas en función de si el DPD se contrata interna o externamente.

4 Funciones del DPD

4.1. Supervisión de la observancia del RGPD

El artículo 39, apartado 1, letra b), encomienda a los DPD, entre otras obligaciones, la de supervisar la observancia del RGPD. El considerando 97 especifica además que, «al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda» del DPD.

Como parte de esas obligaciones de supervisión de la observancia, los DPD pueden, en particular:

- recabar información para determinar las actividades de tratamiento;
- analizar y comprobar la conformidad con la normativa de las actividades de tratamiento;
- informar, asesorar y emitir recomendaciones al responsable o al encargado del tratamiento.

Supervisar la observancia no significa que el DPD sea personalmente responsable de cualquier caso de inobservancia. El RGPD establece claramente que es el responsable y no el DPD quien está obligado a aplicar «medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento» (artículo 24, apartado 1). El cumplimiento de las normas en materia de protección de datos es responsabilidad corporativa del responsable del tratamiento, no del DPD.

4.2. Papel del DPD en una evaluación de impacto relativa a la protección de datos

De conformidad con el artículo 35, apartado 1, es labor del responsable del tratamiento y no del DPD realizar, cuando sea preciso, una evaluación de impacto de las operaciones de tratamiento de datos. No obstante, el DPD puede desempeñar un papel muy importante y útil a la hora de ayudar al responsable del tratamiento. Siguiendo el principio de la protección de datos desde el diseño, al artículo 35, apartado 2, establece específicamente que el responsable del tratamiento «recabará el asesoramiento» del DPD cuando realice una evaluación de impacto relativa a la protección de datos. A su vez, el artículo 39, apartado 1, letra c), impone al DPD la obligación de «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».

El Grupo de Trabajo del artículo 29 recomienda que el responsable del tratamiento busque el asesoramiento del DPD en las siguientes cuestiones, entre otras [35]:

- si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos;
- qué metodología debe seguirse al llevar a cabo una evaluación de impacto;
- si debe realizarse la evaluación de impacto en la propia organización o subcontratarse;
- qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los interesados;

[35] El artículo 39, apartado 1, menciona las funciones del DPD e indica que tendrá «como mínimo» las que a continuación enumera. Por lo tanto, nada impide al responsable del tratamiento asignar al DPD otras funciones aparte de las mencionadas expresamente en el artículo 39, apartado 1, o especificar dichas funciones con más detalle.

- si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con el RGPD.

Si el responsable no está de acuerdo con el asesoramiento ofrecido por el DPD, la documentación de la evaluación de impacto debe justificar específicamente por escrito por qué no se ha tenido en cuenta el consejo[36].

El Grupo de Trabajo del artículo 29 recomienda, además, que el responsable del tratamiento describa con claridad, por ejemplo en el contrato del DPD, pero también en la información facilitada a los empleados y a la dirección (y a otras partes interesadas, cuando sea pertinente), las funciones exactas del DPD y su alcance, en particular con respecto a la realización de evaluaciones de impacto relativas a la protección de datos.

4.3. Cooperación con la autoridad de control y actuación como punto de contacto

De conformidad con el artículo 39, apartado 1, letras d) y e), el DPD deberá «cooperar con la autoridad de control» y «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».

Estas labores hacen referencia al papel de «facilitador» del DPD, mencionado en la introducción de las presentes directrices. El DPD actúa como punto de contacto para facilitar el acceso de la autoridad de control a los documentos y la información necesarias para la realización de las tareas mencionadas en el artículo 57, así como para el ejercicio de sus poderes de investigación, correctivos, de autorización y consultivos mencionados en el artículo 58. Como ya se ha señalado, el DPD está 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 Europea y de los Estados miembros (artículo 38, apartado 5). No obstante, la obligación de mantener el secreto o la confidencialidad no prohíbe al DPD contactar con la autoridad de control y recabar su asesoramiento. El artículo 39, apartado 1, letra e), establece que el DPD podrá realizar consultas a la autoridad de control sobre cualquier otro asunto, en su caso.

4.4. Enfoque basado en el riesgo

El artículo 39, apartado 2, requiere que el DPD desempeñe 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».

Dicho artículo recuerda un principio general y de sentido común, que puede ser pertinente para muchos aspectos del trabajo diario de un DPD. En esencia, requiere que los DPD establezcan prioridades en lo que respecta a sus actividades y centren sus esfuerzos en las cuestiones que presenten mayores riesgos para la protección de datos. Esto no significa que deban desatender la supervisión de

[36] El artículo 24, apartado 1, estipula que «teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar ***y poder demostrar*** que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario».

la observancia de las normas en las operaciones de tratamiento de datos que tengan comparativamente menos riesgos, sino que deben centrarse principalmente en los ámbitos de mayor riesgo.

Este enfoque selectivo y pragmático debe ayudar a los DPD a asesorar al responsable del tratamiento sobre qué metodología usar cuando se realice una evaluación de impacto relativa a la protección de datos, qué ámbitos deben ser objeto de una auditoria de protección de datos interna o externa, qué actividades de formación internas proporcionar al personal o a los directivos encargados de las actividades de protección de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

4.5. Papel del DPD en el mantenimiento de registros

En virtud del artículo 30, apartados 1 y 2, es el responsable o el encargado del tratamiento, y no el DPD, quien está obligado a llevar «un registro de las actividades de tratamiento efectuadas bajo su responsabilidad» o a mantener «un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable».

En la práctica, es frecuente que los DPD elaboren inventarios y mantengan un registro de las operaciones de tratamiento basándose en la información que les proporcionan los distintos departamentos responsables del tratamiento de datos en su organización. Esta práctica se ha establecido en virtud de muchas legislaciones nacionales vigentes y de las normas sobre protección de datos aplicables a las instituciones y organismos de la UE[37].

El artículo 39, apartado 1, establece una lista de tareas mínimas de que debe encargarse el DPD. Por tanto, nada impide que el responsable o el encargado del tratamiento asignen al DPD la tarea de mantener un registro de las operaciones de tratamiento bajo la responsabilidad del responsable o del encargado del tratamiento. Dicho registro debe considerarse una de las herramientas que permiten al DPD realizar sus funciones de supervisión de la observancia de las normas y de información y asesoramiento al responsable o al encargado del tratamiento.

En cualquier caso, el registro que se debe mantener con arreglo al artículo 30 debe considerarse también una herramienta que permita al responsable y a la autoridad de control, si así lo solicitan, tener una perspectiva general de todas las actividades de tratamiento de los datos personales que una organización está llevando a cabo. Es, por tanto, un requisito previo para la observancia de las normas y, como tal, una medida efectiva de rendición de cuentas.

[37] Artículo 24, apartado 1, letra d), del Reglamento (CE) n.º 45/2001.

5 ANEXO - DIRECTRICES RELATIVAS AL DPD: QUÉ DEBO SABER

El objetivo del presente anexo es responder, en un formato simplificado y de fácil lectura, a algunas de las preguntas clave que las organizaciones pueden plantear con respecto a los nuevos requisitos de designación de un DPD en virtud del RGPD.

Designación del DPD

1 ¿Qué organizaciones deben nombrar un DPD?

La designación de un DPD es una obligación:

- si el tratamiento lo lleva a cabo una autoridad u organismo público (con independencia del tipo de datos que se traten);
- si las actividades principales del responsable o del encargado consisten en operaciones de tratamiento que, en razón de su naturaleza, alcance o fines, requieran una observación habitual y sistemática de interesados a gran escala;
- si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales o de datos relativos a condenas e infracciones penales.

Téngase en cuenta que el Derecho de la Unión o de los Estados miembros podrá exigir el nombramiento de DPD también en otras situaciones. Finalmente, aunque la designación de un DPD no sea obligatoria, en ocasiones las organizaciones pueden considerar de utilidad nombrar un DPD de forma voluntaria. El Grupo de Trabajo sobre protección de datos del artículo 29 alienta estos esfuerzos voluntarios. Cuando una organización designe un DPD de forma voluntaria, se aplicarán a su designación, su puesto y sus tareas los mismos requisitos que si el nombramiento hubiera sido obligatorio.

Fuente: Artículo 37, apartado 1, del RGPD

2 ¿Cuál es el significado de «actividades principales»?

Las «actividades principales» pueden considerarse las operaciones clave necesarias para lograr los objetivos del responsable o del encargado del tratamiento. Dichas actividades incluyen también todas aquellas en las que el tratamiento de datos sea una parte indisociable de la actividad del responsable o el encargado del tratamiento. Por ejemplo, el tratamiento de datos relativos a la salud, como historiales de pacientes, debe considerarse una de las actividades principales de cualquier hospital y, por ello, los hospitales deben designar un DPD.

Por otra parte, todas las organizaciones llevan a cabo determinadas actividades, por ejemplo, pagar a sus empleados o realizar actividades ordinarias de apoyo de TI. Dichas actividades son ejemplo de funciones de apoyo necesarias para la actividad principal o el negocio principal de la organización. Aunque estas actividades son necesarias o esenciales, normalmente se consideran funciones auxiliares más que la actividad principal.

Fuente: Artículo 37, apartado 1, letras b) y c), del RGPD

3 ¿Qué significa «a gran escala»?

El RGPD no define qué actividades constituyen un tratamiento a gran escala. El Grupo de Trabajo recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala:

- el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
- el volumen de datos o la variedad de elementos de datos distintos que se procesan;
- la duración o permanencia de la actividad de tratamiento de datos;
- el alcance geográfico de la actividad de tratamiento.

Como ejemplos de tratamiento a gran escala cabe citar:

- el tratamiento de datos de pacientes en el desarrollo normal de la actividad de un hospital;
- el tratamiento de datos de desplazamiento de las personas que utilizan el sistema de transporte público de una ciudad (p. ej. seguimiento a través de tarjetas de transporte);
- el tratamiento de datos de geolocalización a tiempo real de clientes de una cadena internacional de comida rápida con fines estadísticos, por parte de un responsable del tratamiento especializado en la prestación de estos servicios;
- el tratamiento de datos de clientes en el desarrollo normal de la actividad de una compañía de seguros o de un banco;
- el tratamiento de datos personales para la publicidad comportamental por un motor de búsqueda;
- el tratamiento de datos (contenido, tráfico, ubicación) por parte de proveedores de servicios de telefonía o internet;

Como casos que no constituyen tratamiento a gran escala cabe señalar:

- el tratamiento de datos de pacientes por parte de un solo médico;
- el tratamiento de datos personales relativos a condenas e infracciones penales por parte de un abogado.

Fuente: Artículo 37, apartado 1, letras b) y c), del RGPD

4 ¿Qué significa «observación habitual y sistemática»?

La noción de observación habitual y sistemática de los interesados no está definida en el RGPD, pero claramente incluye todas las formas de observación y elaboración de perfiles en internet, inclusive con fines de publicidad comportamental. No obstante, el concepto de observación no se limita al entorno de internet.

Ejemplos de actividades que pueden constituir una observación habitual y sistemática de interesados son: operar una red de telecomunicaciones; prestar servicios de telecomunicaciones; redireccionar correos electrónicos; actividades de mercadotecnia basadas en datos; elaborar de perfiles y otorgar puntuación con fines de evaluación de riesgos (p. ej. para determinar la calificación crediticia, establecer primas de seguros, prevenir el fraude, detectar blanqueo de dinero); llevar a cabo un seguimiento de la ubicación, por ejemplo, mediante aplicaciones móviles; programas de fidelidad; publicidad comportamental; seguimiento de los datos de bienestar, estado físico y salud mediante dispositivos ponibles; televisión de circuito cerrado; dispositivos conectados, como contadores inteligentes, coches inteligentes, domótica, etc.

El Grupo de Trabajo del artículo 29 interpreta «habitual» con uno o más de los siguientes significados:

- continuado o que se produce a intervalos concretos durante un periodo concreto;
- recurrente o repetido en momentos prefijados;
- que tiene lugar de forma constante o periódica.

El Grupo de Trabajo interpreta «sistemático» con uno o más de los siguientes significados:

- que se produce de acuerdo con un sistema;
- preestablecido, organizado o metódico;
- que tiene lugar como parte de un plan general de recogida de datos;
- llevado a cabo como parte de una estrategia.

Fuente: Artículo 37, apartado 1, letra b), del RGPD

5 ¿Pueden las organizaciones nombrar un DPD de forma conjunta? Si es así, ¿en qué condiciones?

Sí. Un grupo empresarial puede designar un único DPD, siempre que este «sea fácilmente accesible desde cada establecimiento». La noción de accesibilidad se refiere a las funciones del DPD como punto de contacto con respecto a los interesados, la autoridad de control y la organización con carácter interno. Con el fin de garantizar que el DPD, ya sea interno o externo, sea accesible, es importante asegurarse de que se dispone de sus datos de contacto. El DPD, con ayuda de un equipo si es necesario, debe estar en condiciones de comunicarse eficazmente con los interesados y cooperar con las correspondientes autoridades de control. Esto significa que dicha comunicación debe tener lugar en el idioma o idiomas utilizados por las autoridades de control y los interesados afectados. La disponibilidad de un DPD (ya sea físicamente en las mismas instalaciones como empleado, ya sea en línea o mediante otros medios seguros de comunicación) es fundamental para garantizar que los interesados puedan contactar con el DPD.

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.

Fuente: Artículo 37, apartados 2 y 3, del RGPD

6 ¿Cuál debe ser la ubicación del DPD?

Para garantizar que el DPD sea accesible, el Grupo de Trabajo del artículo 29 recomienda que el DPD se encuentre en la Unión Europea, con independencia de si el responsable o el encargado del tratamiento está establecido en ella. No obstante, no puede excluirse que en algunas situaciones en las que el responsable o el encargado del tratamiento no tenga establecimiento en la Unión Europea, un DPD pueda llevar a cabo sus actividades de manera más eficaz si se encuentra situado fuera de la Unión Europea.

7 ¿Es posible nombrar un DPD externo?

Sí. El DPD podrá ser un miembro de la plantilla del responsable o el encargado el tratamiento (DPD interno) o desempeñar sus funciones en el marco de un contrato de servicios. Esto significa que el DPD puede ser externo y, en ese caso, su función puede ejercerse sobre la base de un contrato de servicios suscrito con una persona física o una organización.

Cuando la función del DPD la ejerza un proveedor de servicios externo, un grupo de personas que trabaje para dicha entidad podrá desarrollar efectivamente las funciones de DPD como equipo, bajo la responsabilidad de un contacto principal designado como persona «a cargo» del cliente. En ese caso, es fundamental que cada miembro de la organización que ejerza las funciones de DPD cumpla todos los requisitos aplicables del RGPD.

En aras de la claridad jurídica y de la buena organización y con el fin de evitar conflictos de intereses de los miembros del equipo, las directrices recomiendan distribuir de manera clara las tareas dentro del equipo del DPD externo y asignar una única persona como contacto principal y persona «a cargo» de cada cliente.

Fuente: Artículo 37, apartado 6, del RGPD

8 ¿Cuáles son las cualidades profesionales que debería tener un DPD?

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 sus funciones.

El nivel de conocimientos especializados necesario se debe determinar en función de las operaciones de tratamiento de datos realizadas y de la protección exigida para los datos personales tratados. Por ejemplo, cuando la actividad de tratamiento de los datos es especialmente compleja o cuando implica una gran cantidad de datos sensibles, el DPD podría necesitar un nivel mayor de conocimientos y apoyo.

Las competencias y conocimientos pertinentes incluyen:

- conocimientos especializados sobre la legislación y prácticas nacionales y europeas en materia de protección de datos y una profunda comprensión del RGPD;
- comprensión de las operaciones de tratamiento que se llevan a cabo;
- comprensión de las tecnologías de la información y de la seguridad de los datos;
- conocimiento del sector empresarial y de la organización;
- capacidad para fomentar una cultura de protección de datos dentro de la organización.

Fuente: Artículo 37, apartado 5, del RGPD

9 ¿Qué recursos debe asignar al DPD el responsable o el encargado del tratamiento?

El DPD debe contar con los recursos necesarios para poder realizar sus funciones.

Dependiendo de la naturaleza de las actividades de tratamiento y de la actividad y el tamaño de la organización, se deberán asignar los siguientes recursos al DPD:

- apoyo activo al DPD por parte de la alta dirección;
- tiempo suficiente para que el DPD cumpla con sus funciones;
- apoyo adecuado en cuanto a recursos financieros, infraestructura (locales, instalaciones, equipos) y personal según se requiera;
- comunicación oficial de la designación del DPD a toda la plantilla;
- acceso a otros servicios dentro de la organización de modo que los DPD puedan recibir apoyo esencial, datos e información de dichos servicios;
- formación continua.

Fuente: Artículo 38, apartado 2 del RGPD

10 ¿Cuáles son las garantías que permiten al DPD desempeñar sus funciones de manera independiente? ¿Cuál es el significado de «conflicto de intereses»?

Existen diversas salvaguardias que permiten al DPD actuar de manera independiente:

- el DPD no recibirá instrucciones por parte de los responsables o encargados del tratamiento en lo relativo al ejercicio de sus funciones como DPD;
- no podrá ser sancionado o destituido por el responsable del tratamiento por el desempeño de sus funciones;
- no habrá conflictos de intereses con otras posibles funciones y obligaciones.

Las otras funciones y obligaciones de un DPD no deben llevar a un conflicto de intereses. Esto significa, en primer lugar, que el DPD no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso.

Como norma general, los cargos en conflicto dentro de una organización pueden incluir los puestos de alta dirección (tales como director general, director de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI) pero también otros cargos inferiores en la estructura organizativa si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento. Asimismo, también puede surgir un conflicto de intereses, por ejemplo, si se pide a un DPD que represente al responsable o encargado del tratamiento ante los tribunales en casos relacionados con la protección de datos.

Fuente: Artículo 38, apartados 3 y 6, del RGPD

11 ¿Qué significa «supervisión de la observancia»?

Como parte de esas obligaciones de supervisión de la observancia, los DPD pueden, en particular:

- recabar información para determinar las actividades de tratamiento;
- analizar y comprobar la conformidad con la normativa de las actividades de tratamiento;
- informar, asesorar y emitir recomendaciones al responsable o al encargado del tratamiento.

Fuente: Artículo 39, apartado 1, letra b), del RGPD

12 ¿Es el DPD responsable personalmente del incumplimiento de los requisitos de protección de datos?

No, el DPD no es responsable personalmente del incumplimiento de los requisitos de protección de datos. Es el responsable o el encargado del tratamiento quien está obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza de conformidad con el RGPD. El cumplimiento de las normas en materia de protección de datos es responsabilidad del responsable del tratamiento.

13 ¿Cuál es el papel del DPD con respecto a las evaluaciones de impacto relativas a la protección de datos y al registro de las actividades de tratamiento?

En cuanto a las evaluaciones de impacto relativas a la protección de los datos, el responsable o el encargado del tratamiento debe recabar el asesoramiento del DPD sobre, entre otras, las siguientes cuestiones:

- si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos;
- qué metodología debe seguirse al llevar a cabo una evaluación de impacto;
- si debe realizarse la evaluación de impacto en la propia organización o subcontratarse;
- qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los interesados;
- si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con los requisitos de la protección de datos.

En cuanto a los registros de las actividades de tratamiento, es obligación del responsable o del encargado del tratamiento, y no del DPD, mantener los registros de las operaciones de tratamiento. No obstante, nada impide que el responsable o el encargado del tratamiento asignen al DPD la tarea de mantener un registro de las operaciones de tratamiento bajo la responsabilidad del responsable o del encargado del tratamiento. Dicho registro debe considerarse una de las herramientas que permiten al DPD realizar sus funciones de supervisión de la observancia de la normativa y de información y asesoramiento al responsable o al encargado del tratamiento.

Fuente: Artículo 39, apartado 1, letra c), y artículo 30 del RGPD

Hecho en Bruselas, a 13 de diciembre de 2016

Por el Grupo de Trabajo
La Presidenta

Isabelle FALQUE-PIERROTIN

Revisado por última vez y adoptado el 5 de abril de 2017

Por el Grupo de Trabajo
La Presidenta

Isabelle FALQUE-PIERROTIN