GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS

16/EN
GT 243

Directrices sobre los delegados de la protección de datos (DPD)

Adoptado el 13 de diciembre de 2016

Este Grupo de Trabajo se creó de conformidad con el artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos y privacidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva 2002/58/CE.

De su secretaría se ocupa la Dirección C (Derechos fundamentales y Estado de derecho) de la Comisión Europea, Dirección General de Justicia y Consumidores, Bruselas B-1049, Bélgica, Despacho n.º MO59 02/27.

Sitio web: http://ec.europa.eu/justice/data-protection/index_en.htm

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

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

teniendo en cuenta los artículos 29 y 30 de la misma,

teniendo en cuenta sus Normas de procedimiento,

HA ADOPTADO LAS SIGUIENTES DIRECTRICES:

Índice

1 Introducción

La Normativa general de protección de datos («NGPD»)[1], cuya entrada en vigor está prevista el 25 de mayo de 2018, ofrecerá un marco de cumplimiento modernizado basado en la rendición de cuentas por lo que se refiere a la protección de datos en Europa. Los delegados de la protección de datos (DPD) serán el elemento nuclear de este nuevo marco jurídico para muchas organizaciones, lo que facilita el cumplimiento de las disposiciones de la NGPD.

Según la NGPD, será obligado para determinados responsables y encargados del tratamiento de datos la designación de un DPD[2], lo que será aplicable a todas las autoridades y organismos públicos (con independencia de los datos que procesen) y a otras organizaciones que, como actividad principal, realicen un seguimiento de personas de forma sistemática y a gran escala, o que procesen categorías especiales de datos personales a gran escala.

Incluso en los casos en los que la NGPD no requiera específicamente el nombramiento de un DPD, las organizaciones puede que en ocasiones consideren útil designar un DPD de forma voluntaria. El Grupo de Trabajo del Artículo 29 (GP29) anima a llevar a cabo estos esfuerzos voluntarios.

El concepto del DPD no es nuevo. Si bien 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 de la NGPD, el GP29 argumentaba que el DPD es la piedra angular de la rendición de cuentas y que el nombramiento de un DPD puede facilitar el cumplimiento de la normativa y, por otra parte, convertirse en una ventaja competitiva para las empresas[4]. Además de facilitar el cumplimiento mediante la implementación de herramientas de rendición de cuentas (tales como facilitar o llevar a cabo evaluaciones de impacto y auditorías de protección de datos), los DPD actúan de intermediarios entre las partes interesadas correspondientes (p. ej. autoridades supervisoras, interesados y unidades de negocio dentro de las organizaciones).

Los DPD no son personalmente responsables en caso de incumplimiento de la NGPD. La NGPD declara taxativamente que es el responsable o el encargado del tratamiento quien está obligado a garantizar y poder demostrar que el tratamiento se lleva a cabo con arreglo a sus disposiciones (artículo 24(1)). La protección de datos es responsabilidad del responsable o el encargado del tratamiento,

quien asimismo tiene un papel crucial a la hora de hacer posible el desempeño efectivo de las tareas del DPD. El nombramiento de un DPD es el primer paso, pero debe conferírsele suficiente autonomía y recursos para que lleve a cabo su cometido de forma efectiva.

---

[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) (OJ L 119, 4.5.2016).

[2] El nombramiento de un DPD es también obligatorio para las autoridades competentes según el 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 (OJ L 119, 4.5.2016, p. 89–131), así como la legislación nacional de aplicación. Aunque estas directrices se centran en los DPD según la NGPD, la orientación es pertinente también por lo que se refiere a los DPD según la Directiva 2016/680, con respecto a 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 (OJ L 281, 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

La NGPD reconoce al DPD como un actor clave en el nuevo sistema de gestión de los datos y establece las condiciones de su nombramiento, su puesto y sus tareas. El objeto de estas directrices es aclarar las disposiciones relevantes de la NGPD para ayudar a los responsables y encargados del tratamiento a cumplir con la legislación y, asimismo, ayudar a los DPD en el desempeño de su función. Las directrices ofrecen también recomendaciones de mejores prácticas a partir de la experiencia acumulada en algunos Estados miembros de la UE. El GP29 hará un seguimiento de la puesta en práctica de estas directrices y podrá complementarlas con detalles adicionales según proceda.

2 Designación de un DPD

2.1. Designación obligatoria

El artículo 37(1) de la NGPD exige que se designe un DPD en tres casos específicos[5]:

a) cuando el tratamiento lo lleva a cabo una autoridad u organismo públicos[6];
b) cuando las actividades principales del responsable o el encargado del tratamiento consisten en operaciones de tratamiento que requieren el seguimiento regular y sistemático de los interesados a gran escala; o
c) cuando las actividades principales del responsable o el encargado del tratamiento consisten en el tratamiento a gran escala de categorías especiales de datos[7] o[8] datos personales relacionados con condenas y delitos penales[9].

En las siguientes subsecciones, el GP29 ofrece orientación en relación con los criterios y la terminología usados en el artículo 37(1).

A menos que resulte obvio que una organización no requiere designar un DPD, el GP29 recomienda que los responsables y encargados del tratamiento documenten el análisis interno llevado a cabo para determinar si debe nombrarse o no un DPD a fin de poder demostrar que se han tenido en cuenta adecuadamente los factores pertinentes[10].

Cuando una organización designe un DPD de forma voluntaria, se aplicarán a su designación, su puesto y sus tareas los mismos requisitos establecidos en los artículos 37 a 39 que si la designación hubiese sido obligatoria.

Esto no es óbice para que una organización que no desee designar un DPD de forma voluntaria y no esté legalmente obligada a designar un DPD emplee a pesar de todo a personal específico o consultores externos con tareas relacionadas con la protección de datos personales. En este caso es importante asegurar que no haya confusión posible relativa a su cargo, estatus, puesto y tareas.

Por lo tanto, debe dejarse en 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 cargo de esta persona o asesor no es el de DPD[11]. [11]

---

[5] Obsérvese que, según el artículo 37(4), la legislación de la Unión o de los Estados miembros podrá exigir la designación de DPD también en otras situaciones.

[6] Salvo por lo que respecta a tribunales que actúen en su ámbito de competencia.

[7] De conformidad con el artículo 9, estas incluyen datos personales que revelen el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas o la pertenencia a sindicatos, así como el tratamiento de datos genéticos, datos biométricos para la identificación exclusiva de personas físicas, datos relativos a la salud o datos referentes a la vida sexual o la orientación sexual de las personas.

[8] El artículo 37(1)(c) usa la palabra «y». Véase en el apartado 2.1.5 a continuación la explicación sobre el uso de «o» en vez de «y».

[9] Artículo 10.

[10] Véase el artículo 24(1).

[11] Esto es relevante también por lo que se refiere a los directores de privacidad (CPO, por sus siglas en inglés) 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 de la NGPD, por ejemplo, en cuanto a los recursos disponibles o las garantías de independencia, y por consiguiente, no pueden considerarse ni hacerse mención a ellos como DPD.

2.1.1 «AUTORIDAD U ORGANISMO PÚBLICOS»

La NGPD no define lo que constituye una «autoridad u organismo públicos». El GP29 considera que tal noción debe determinarse según la legislación de cada país. Por consiguiente, las autoridades y organismos públicos incluyen a las autoridades nacionales, regionales y locales, pero el concepto, conforme a las legislaciones nacionales aplicables, también suele incluir una serie de otros organismos regidos por el derecho público[12]. En tales casos, la designación de un DPD es obligatoria.

Una tarea pública se puede llevar a cabo, y la autoridad pública se puede ejercer[13], no solo por parte de autoridades u organismos públicos sino de otras personas físicas o jurídicas regidas por el derecho público o privado en sectores tales como, de acuerdo con la legislación nacional de cada Estado miembro, los servicios de transporte público, el suministro de agua y energía, la infraestructura viaria, la radiodifusión pública, la vivienda pública o los organismos disciplinarios para las profesiones reguladas.

En estos casos, los interesados pueden hallarse en una situación muy similar a cuando sus datos son procesados por una autoridad u organismo públicos. En concreto, los datos pueden tratarse para fines similares y, asimismo, las personas suelen tener pocas opciones o ninguna sobre la manera en que se procesarán sus datos y puede que, por lo tanto, requieran la protección adicional que puede aportar la designación de un DPD.

Aunque no existe obligación en tales casos, el GP29 recomienda, como buena práctica, que:

- las organizaciones privadas que llevan a cabo tareas o ejercen autoridad pública designen un DPD y que
- la actividad de dicho DPD cubra también todas las operaciones de tratamiento llevadas a cabo, incluidas las que no están relacionadas con el desempeño de una tarea pública o el ejercicio de una función pública (p. ej. la gestión de una base de datos de empleados).

2.1.2 «ACTIVIDADES PRINCIPALES»

Los apartados 1, b y c del artículo 37 de la NGPD se refieren a las «actividades principales del responsable o el encargado del tratamiento». El considerando 97 especifica que las actividades principales de un responsable del tratamiento están relacionadas con «actividades primarias y no 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 el encargado del tratamiento.

No obstante, el término «actividades principales» no debe interpretarse excluyendo aquellas actividades en las que el tratamiento de datos forme parte intrínseca de la actividad del responsable o el encargado del tratamiento. Por ejemplo, la actividad principal de un hospital es la prestación de cuidados sanitarios, pero un hospital no podría proporcionar cuidados sanitarios de forma segura y eficaz sin procesar datos de salud, como son los registros de salud de los pacientes.

---

[12] Véase, p. ej., la definición de «organismo del sector público» y «organismo regido por el Derecho público» en los apartados 1 y 2 del artículo 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 (OJ L 345, 31.12.2003, p. 90).

[13] Artículo 6(1)(e).

Por lo tanto, el tratamiento de estos datos debe considerarse que forma parte de las actividades principales de cualquier hospital y, por consiguiente, los hospitales deben designar un DPD.

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

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

2.1.3 «A GRAN ESCALA»

Los apartados b y c del artículo 37(1) determinan que el tratamiento de los datos personales debe llevarse a cabo a gran escala para poner en marcha la designación de un DPD. La NGPD no define lo que constituye «a gran escala», si bien el considerando 91 ofrece alguna orientación a este respecto[14].

De hecho, no es posible señalar una cifra exacta ya sea con relación a la cantidad de datos procesados como al número de personas afectadas, que sería aplicable en todas las situaciones. Esto no excluye la posibilidad, no obstante, de que con el tiempo pueda desarrollarse un método estándar para especificar en términos objetivos y cuantitativos lo que constituiría «a gran escala» respecto de determinados tipos de actividades de tratamiento comunes. El GP29 prevé también contribuir a este desarrollo compartiendo y publicando ejemplos de los umbrales pertinentes para la designación de un DPD.

En cualquier caso, el GP29 recomienda que se tengan en cuenta los siguientes factores, en especial, a la hora de determinar si el tratamiento se lleva a cabo a gran escala:

- El número de interesados involucrados —bien como cifra concreta o como proporción de la población correspondiente—
- El volumen de datos o el abanico de diferentes conceptos de datos que se procesan
- La duración, o permanencia, de la actividad de tratamiento de datos
- El alcance geográfico de la actividad de tratamiento

[14] Según el considerando, se incluiría en especial las «operaciones de tratamiento a gran escala que tengan por objeto procesar una cantidad considerable de datos personales en el ámbito regional, nacional o supranacional, que pudieran afectar a un gran número de interesados y que sean susceptibles de generar un riesgo elevado». Por otra parte, el considerando señala específicamente que «no debe considerarse que el tratamiento de datos personales se realiza a gran escala si el tratamiento concierne a datos personales de pacientes o clientes a cargo de un médico, otro profesional sanitario o un abogado». Es importante considerar que, si bien el considerando ofrece ejemplos situados en los extremos de la escala (tratamiento por parte de un médico frente al tratamiento de datos en la totalidad de un país o en toda Europa), hay una gran zona gris entre ambos extremos. Debe tenerse en cuenta, además, que este considerando se refiere a evaluaciones de impacto de la protección de datos, lo que implica que algunos elementos podrían ser específicos de ese contexto y no se aplican necesariamente a la designación de DPD exactamente del mismo modo.

Son ejemplos de tratamiento a gran escala los siguientes:

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

Casos que no constituyen tratamiento a gran escala son los siguientes:

- tratamiento de datos de pacientes por parte de un médico
- tratamiento de datos personales relativos a condenas y delitos penales por parte de un abogado

2.1.4 «SEGUIMIENTO REGULAR Y SISTEMÁTICO»

La noción de seguimiento regular y sistemático de interesados no está definida en la NGPD, pero el concepto de «seguimiento del comportamiento de interesados» se menciona en el considerando 24[15] e incluye claramente todas las formas de seguimiento y creación de perfiles en Internet, inclusive a efectos de publicidad basada en el comportamiento.

No obstante, la noción de seguimiento no está limitada al entorno *on-line* y el seguimiento en Internet solo debe considerarse un ejemplo de seguimiento del comportamiento de los interesados[16].

El GP29 interpreta «regular» con algunos de los siguientes significados:

- Continuado o que se produce a intervalos concretos durante un periodo concreto
- Recurrente o repetido en momentos prefijados
- Que se produce de forma constante o periódica

El GP29 interpreta «sistemático» con algunos 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

[15] «Para determinar si puede considerarse que una actividad de tratamiento hace el seguimiento del comportamiento de los interesados, debe esclarecerse si se realiza el seguimiento de personas físicas en Internet, incluyendo el uso posterior potencial de técnicas de tratamiento de datos personales consistentes en la creación de perfiles personales, especialmente para tomar decisiones relativas a dicha persona o para analizar o predecir sus preferencias personales, sus comportamientos y sus actitudes.»

[16] Obsérvese que el considerando 24 se centra en la aplicación extraterritorial de la NGPD. Existe además otra diferencia entre la expresión «seguimiento de su comportamiento» (artículo 3(2) (b)) y «seguimiento regular y sistemático de los interesados» (artículo 37(1)(b)), por lo que podría considerarse que constituyen conceptos distintos.

Ejemplos: operar una red de telecomunicaciones; prestar servicios de telecomunicaciones; redireccionar correo electrónico; creación de perfiles y puntuación con fines de evaluación de riesgos (p. ej. con fines de puntuación crediticia, establecimiento de primas de seguros, prevención del fraude, detección de blanqueo de dinero); seguimiento de ubicación, por ejemplo, mediante aplicaciones móviles; programas de fidelización; publicidad basada en el comportamiento; seguimiento de datos de bienestar, estado físico y salud mediante dispositivos portátiles; circuito cerrado de televisión; dispositivos conectados, p. ej. contadores inteligentes, coches inteligentes, domótica, entre otros.

2.1.5 CATEGORÍAS ESPECIALES DE DATOS Y DATOS RELATIVOS A CONDENAS Y DELITOS PENALES

El artículo 37(1)(c) aborda el tratamiento de categorías especiales de datos con arreglo al artículo 9, así como datos personales relativos a condenas y delitos penales expuestos en el artículo 10. Si bien la disposición emplea la palabra «y», no existe una política determinada para la aplicación simultánea de ambos criterios. Por lo tanto, debe considerarse que el texto dice «o».

2.2. DPD del encargado del tratamiento

El artículo 37 se aplica tanto a los responsables[17] como a los encargados del tratamiento[18] con respecto a la designación de un DPD. En función de quién cumpla los criterios sobre la designación obligatoria, en algunos casos solo el responsable o solo el encargado, en otros casos tanto el responsable como el encargado estarán obligados a nombrar un DPD (los cuales deberán cooperar entre sí).
Es importante destacar que, incluso si el responsable del tratamiento cumple los criterios para la designación obligatoria, su encargado del tratamiento no está necesariamente obligado a nombrar un DPD, aunque puede ser una práctica aconsejable.

Ejemplos:

- una pequeña empresa familiar que se dedica a la distribución de electrodomésticos en una sola ciudad usa los servicios de un responsable de tratamiento cuya actividad principal es prestar servicios de análisis de sitios web y asistencia mediante publicidad y marketing selectivos. Las actividades de la empresa familiar y sus clientes no generan ningún tratamiento de datos «a gran escala», teniendo en cuenta el reducido número de clientes y sus actividades relativamente limitadas. Sin embargo, las actividades del responsable del tratamiento, al contar con muchos clientes como esta pequeña empresa, consideradas en conjunto, suponen un tratamiento de datos a gran escala. Por consiguiente, el responsable del tratamiento debe designar un DPD según el artículo 37(1)(b). Al mismo tiempo, la empresa familiar en sí no está sujeta a la obligación de designar un DPD.
- Una empresa fabricante de azulejos mediana subcontrata sus servicios de salud ocupacional a un responsable de tratamiento externo, que tiene un gran número de clientes similares. El encargado del tratamiento designará un DPD según el artículo 37(1)(c), siempre que el tratamiento se realice a gran escala. Sin embargo, el fabricante no está sujeto necesariamente a la obligación de designar un DPD.

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

[18] El encargado del tratamiento se define en el artículo 4(8) como la persona u organismo que procesa los datos en nombre del responsable.

En aras de las buenas prácticas, el GP29 recomienda que el DPD designado por un encargado del tratamiento supervise también las actividades llevadas a cabo por la organización del encargado cuando actúe como responsable del tratamiento por derecho propio (p. ej. RR HH, TI o logística).

2.3. «Fácilmente accesible desde cada establecimiento»

El artículo 37(2) permite a un grupo de empresas 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 respecto de los interesados[19] y la autoridad supervisora[20], pero también internamente dentro de la organización, teniendo en cuenta que una de las tareas del DPD es «informar y asesorar al responsable y el encargado del tratamiento así como a los empleados que llevan a cabo el tratamiento sobre sus obligaciones con arreglo al presente Reglamento[21]».

Para garantizar que el DPD, ya sea interno o externo, sea accesible, es importante asegurarse de que sus datos de contacto estén disponibles de acuerdo con los requisitos de la NGPD[22].

Dicha persona debe estar en condiciones de comunicarse de forma eficaz con los interesados[23] y cooperar[24] con las autoridades supervisoras pertinentes. Esto significa también que esta comunicación debe producirse en el idioma o idiomas usados por las autoridades supervisoras y los interesados correspondientes.

Según el artículo 37(3), puede designarse un único DPD para varias autoridades u organismos públicos, teniendo en cuenta su estructura organizativa y el tamaño. Las mismas consideraciones valen por lo que se refiere a los recursos y la comunicación. Dado que el DPD es responsable de una diversidad de tareas, el responsable del tratamiento debe garantizar que un solo DPD pueda llevarlas a cabo de forma eficiente pese a ser responsable de varias autoridades y organismos públicos.

La disponibilidad personal de un DPD (bien físicamente en los mismos locales como empleado, a través de una línea directa o mediante otros medios de comunicación seguros) es esencial para garantizar que los interesados puedan ponerse en contacto con el DPD. El DPD está obligado a mantener secreto documental y confidencialidad en relación con el desempeño de sus tareas, de acuerdo con el Derecho de la Unión Europea o de los Estados miembros (Artículo 38(5)). No obstante, la obligación de secreto/confidencialidad no prohíbe al DPD entrar en contacto con la autoridad supervisora o pedirle asesoramiento.

2.4. Conocimientos y destrezas del DPD

[19] Artículo 38(4): «los interesados pueden ponerse en contacto con el delegado de la protección de datos en relación con todas las cuestiones concernientes al tratamiento de sus datos personales y para ejercer sus derechos según el presente Reglamento».

[20] Artículo 39(1)(e): «actuar como punto de contacto para la autoridad supervisora respecto de todas las cuestiones relacionadas con el tratamiento, incluida la consulta previa a la que hace referencia el artículo 36 y consultar, cuando sea pertinente, en relación con cualquier otro asunto».

[21] Artículo 39(1)(a).

[22] Véase también el siguiente apartado 2.5.

[23] Artículo 12(1): *«El responsable del tratamiento tomará las medidas pertinentes para proporcionar la información a la que hacen referencia los artículos 13 y 14 y toda comunicación según los artículos 15 a 22 y 34 en relación con el tratamiento al interesado en un formulario conciso, transparente, inteligible y fácilmente accesible, empleando un lenguaje claro y sencillo, en particular para toda información que se dirija específicamente a un niño».*

[24] Artículo 39(1)(d)*: «cooperar con la autoridad supervisora».*

El artículo 37(5) estipula que el DPD «se designará en función de su cualificación profesional y, en especial, su conocimiento experto de la legislación y las prácticas de protección de datos así como su capacidad de desempeñar las tareas a las que hace referencia el artículo 39». El considerando 97 establece que debe determinarse el nivel necesario de conocimiento experto de acuerdo con las operaciones de tratamiento de datos llevadas a cabo y la protección requerida para los datos personales que se están tratando.

- **Nivel de conocimiento**

El nivel de conocimiento requerido no está definido estrictamente pero debe ser acorde con el carácter sensible, la complejidad y la cantidad de datos que procesa una organización. Por ejemplo, cuando una actividad de tratamiento de datos es especialmente compleja, o cuando implica una gran cantidad de datos sensibles, el DPD podrá requerir un nivel mayor de conocimiento y apoyo. Existe también una diferencia dependiendo de si la organización transfiere sistemáticamente datos personales fuera de la Unión Europea o si tales transferencias son ocasionales. Así pues, el DPD debe elegirse con cuidado, teniendo en cuenta debidamente los problemas de protección de datos que surjan dentro de la organización.

- **Cualificación profesional**

Aunque el artículo 37(5) no especifica la cualificación profesional que debe tenerse en cuenta al designar un DPD, un aspecto importante es que los DPD deben tener conocimiento de las leyes y prácticas de protección de datos tanto nacionales como europeas y una comprensión profunda de la NGPD. Resulta útil también que las autoridades supervisoras promuevan una formación adecuada y regular para los DPD.

Es de utilidad el conocimiento que el responsable del tratamiento tenga del sector empresarial y la organización. El DPD debe tener suficiente comprensión de las operaciones de tratamiento llevadas a cabo y los sistemas de información, así como las necesidades de seguridad y protección de los datos del responsable del tratamiento.

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

- **Capacidad de desempeño de sus tareas**

La capacidad de desempeño de las tareas propias del DPD debe medirse tanto por sus cualidades personales y sus conocimientos como por el 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 hacer posible el cumplimiento de la NGPD. El DPD desempeña un papel clave a la hora de promover una cultura de protección de datos dentro de la organización y ayuda a implementar elementos esenciales de la NGPD, como son los principios del tratamiento de datos[25], los derechos de los interesados[26], la protección de datos por diseño y por defecto[27], los registros de actividades de tratamiento[28], la seguridad del tratamiento[29] y la notificación y comunicación de violaciones de datos[30].

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

- **DPD en función de un contrato de servicios**

La función del DPD puede ejercerse también sobre la base de un contrato de servicios suscrito con una persona física o una organización ajena a la organización del responsable o el encargado del tratamiento. En este último caso, es esencial que cada miembro de la organización que ejerza las funciones de un DPD cumpla todos los requisitos pertinentes expuestos en la sección 4 de la NGPD (p. ej., es esencial que nadie tenga un conflicto de interés). Es igualmente importante que cada miembro que ocupe dicho puesto esté protegido por las disposiciones de la NGPD (p. ej. que impidan la rescisión injustificada del contrato de servicios por las actividades del DPD así como el despido improcedente de cualquier miembro de la organización que lleve a cabo las tareas de DPD). Al mismo tiempo, es posible combinar las destrezas y puntos fuertes individuales de forma que varias personas, trabajando en equipo, podrán servir de modo más eficiente a sus clientes.

En aras de la claridad legal y la buena organización, se recomienda tener una asignación clara de tareas dentro del equipo del DPD y asignar a una sola persona la función de contacto principal y persona «a cargo» de cada cliente. Por lo general, también sería útil especificar estos puntos en el contrato de servicios.

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

El artículo 37(7) de la NGPD exige que el responsable o el encargado del tratamiento:

- publique los datos de contacto del DPD y
- comunique los datos de contacto a las autoridades supervisoras correspondientes.

El objetivo de estos requerimientos es garantizar que los interesados (tanto dentro como fuera de la organización) y las autoridades supervisoras puedan ponerse en contacto de forma fácil, directa y confidencial con el DPD sin tener que contactar con otra parte de la organización.
Los datos de contacto del DPD deben incluir información que permita a los interesados y a las autoridades supervisoras comunicarse con el DPD de forma fácil (una dirección postal, un número de teléfono específico y una dirección de correo electrónico específica). Cuando corresponda, a efectos de comunicación con el público, podrían disponerse 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(7) no estipula que los datos de contacto publicados deban incluir el nombre del DPD. Aunque hacerlo es una práctica recomendable, le corresponde al responsable del tratamiento y al DPD decidir si es necesario o útil en cada circunstancia concreta[31].
En aras de las buenas prácticas, el GP29 recomienda que las organizaciones comuniquen a la autoridad supervisora y a los empleados el nombre y los 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.

[31] Hay que reseñar que el artículo 33(3)(b), que describe la información que debe proporcionarse a la autoridad supervisora y a los interesados en caso de una violación de datos personales, a diferencia del artículo 37(7), requiere de modo específico que se comunique también el nombre (y no solo los datos de contacto) del DPD.

3 Puesto del DPD

3.1. Implicación del DPD en todas las cuestiones relacionadas con la protección de datos personales

El artículo 38 de la NGPD estipula que el responsable y el encargado del tratamiento deberán garantizar que el DPD «se involucre, de manera adecuada y oportuna, en todas las cuestiones que guarden relación con la protección de los datos personales».

Es crucial que el DPD se involucre desde la fase más temprana posible en todas las cuestiones relacionadas con la protección de datos. En relación con las evaluaciones de impacto de la protección de datos, la NGPD establece expresamente la implicación temprana del DPD y especifica que el responsable del tratamiento deberá solicitar asesoramiento al DPD cuando lleve a cabo tales evaluaciones de impacto[32]. Garantizar que se informe y se consulte al DPD desde el inicio facilitará el cumplimiento de la NGPD, asegurará un enfoque de privacidad por diseño y, por lo tanto, debería ser un procedimiento estándar dentro de la gestión de una organización. Además, es importante que el DPD se perciba como un interlocutor dentro de la organización y que forme parte de los grupos de trabajo pertinentes que se ocupan de las actividades de tratamiento de datos dentro de la organización.

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

- Se invite al DPD a participar con regularidad en reuniones con los cuadros directivos altos y medios.
- Se recomienda que esté presente cuando se tomen decisiones con implicaciones para la protección de datos. Toda la información relevante deberá transmitirse al DPD de manera oportuna para que pueda prestar un asesoramiento adecuado.
- La opinión del DPD deberá siempre gozar de la consideración debida. En caso de desacuerdo, el GP29 recomienda, como buena práctica, documentar las razones de no seguir el consejo del DPD.
- Deberá consultarse con prontitud al DPD una vez que se produzca una violación de datos u otro incidente.

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

3.2. Recursos necesarios

El artículo 38(2) de la NGPD estipula que la organización debe respaldar a su DPD «proporcionando los recursos necesarios para que lleve a cabo sus tareas y acceda a los datos personales y las operaciones de tratamiento, así como para mantener su conocimiento experto». Deben tenerse en cuenta, en especial, los siguientes aspectos:

- Apoyo activo a la función del DPD por parte de la alta dirección (como puede ser el consejo de administración).

  Tiempo suficiente para que los DPD cumplan con sus funciones. Esto es especialmente importante cuando se designa al DPD a tiempo parcial o cuando el empleado lleva a cabo la protección de datos además de otras funciones. De otro modo, las prioridades en conflicto podrían dar lugar al descuido de las obligaciones del DPD. Contar con tiempo suficiente que dedicar a las tareas del DPD es de la máxima importancia. Es una práctica recomendable establecer un porcentaje de tiempo para la función del DPD cuando no se lleve a cabo a tiempo completo. Es también recomendable determinar el tiempo necesario para llevar a cabo la función, el nivel de prioridad apropiado para las funciones del DPD, y para que el DPD (o la organización) redacte un plan de trabajo.

[32] Artículo 35(2).

- Apoyo adecuado en cuanto a recursos económicos, infraestructura (locales, instalaciones, equipos) y personal donde sea pertinente.
- Comunicación oficial de la designación del DPD a todo el personal para asegurar que su existencia y su función se conozcan dentro de la organización.
- Acceso necesario a otros servicios, tales como recursos humanos, departamento jurídico, TI, seguridad, etcétera, de modo que los DPD puedan recibir apoyo esencial, datos e información de esos otros servicios.
- Formación continua. Debe darse a los DPD la oportunidad de mantenerse al corriente de todos los avances que se den en el ámbito de la protección de datos. El objetivo debe ser aumentar constantemente el nivel de conocimiento de los DPD, por lo que se les debe animar a participar en cursos de formación sobre protección de datos y otras formas de desarrollo profesional, como participación en foros sobre privacidad, talleres, etcétera.
- En función del tamaño y la estructura de la organización, puede que sea necesario establecer un equipo del DPD (un DPD y su personal). En tales casos, la estructura interna del equipo así como las tareas y responsabilidades de cada uno de sus miembros deben delimitarse claramente. Del mismo modo, cuando la función del DPD la ejerza un proveedor de servicios externo, un equipo de personas que trabaje para dicha entidad podrá llevar a cabo de hecho las tareas de un DPD a modo de 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 dotarse de forma efectiva con recursos suficientes en relación con el tratamiento de datos que se esté llevando a cabo.

3.3. Instrucciones y «actuación independiente»

El artículo 38(3) establece unas garantías básicas para ayudar a asegurar que los DPD puedan llevar a cabo sus tareas con el suficiente grado de autonomía dentro de su organización. En especial, los responsables y encargados del tratamiento están obligados a garantizar que el DPD «no reciba ninguna instrucción relativa al ejercicio de sus tareas». El considerando 97 añade que los DPD, «sean o no un empleado del responsable del tratamiento, deben estar en condiciones de desempeñar sus tareas y funciones con total independencia».

Esto significa que, en el desempeño de sus tareas según el artículo 39, los DPD no deben recibir instrucciones sobre el modo de ocuparse de un asunto, por ejemplo, sobre el resultado que debe alcanzarse, sobre el modo de investigar una queja o sobre si debe consultarse a la autoridad supervisora. Asimismo, no deben recibir instrucciones de adoptar una determinada postura sobre una cuestión relacionada con la legislación de protección de datos, por ejemplo, una interpretación concreta de la ley. La autonomía de los DPD no significa, sin embargo, que tengan la potestad de tomar decisiones que vayan más allá de sus funciones definidas con arreglo al artículo 39.

El responsable o el encargado del tratamiento sigue siendo el responsable del cumplimiento de la ley de protección de datos y debe poder demostrarlo[33]. Si el responsable o el encargado toma decisiones que sean incompatibles con la NGPD y el consejo del DPD, deberá darse la posibilidad al DPD de expresar con claridad su opinión disconforme ante los responsables de dichas decisiones.

[33] Artículo 5(2).

3.4. Destitución o sanción por realizar tareas de DPD

El artículo 38(3) también establece que los DPD «no deben ser destituidos ni penalizados por el responsable o el encargado del tratamiento por llevar a cabo sus funciones».

Por otra parte, este requisito refuerza la autonomía de los DPD y ayuda a garantizar que actúen con independencia y gocen de suficiente protección en el desempeño de sus funciones de protección de datos.

Las sanciones solo están prohibidas según la NGPD si se imponen como resultado del desempeño por parte del DPD de sus funciones definidas. Por ejemplo, un DPD puede que considere que un tratamiento concreto es susceptible de causar un riesgo elevado y aconseja al responsable o el encargado que lleve a cabo una evaluación de impacto de la protección de datos pero el responsable o el encargado no está de acuerdo con la evaluación del DPD. En un caso así, el DPD no puede ser destituido por expresar este consejo.

Las sanciones pueden adoptar diversas formas y pueden ser directas o indirectas. Pueden consistir, por ejemplo, en la falta de ascensos o su dilación, en impedir la promoción profesional o en negar prestaciones que otros empleados reciben. No es necesario que estas sanciones se lleven a cabo de forma efectiva, su mera amenaza es suficiente siempre que se usen para penalizar al DPD por motivos relacionados con sus actividades.

Como norma general de gestión y como sería el caso para cualquier otro empleado o contratista sujeto a la legislación contractual, laboral o penal aplicable de cada país, un DPD podría ser despedido legítimamente por causas distintas al desempeño de sus funciones como DPD (por ejemplo, en caso de robo, acoso físico, psicológico o sexual u otras faltas graves de conducta similares).

En este contexto, debe señalarse que la NGPD no especifica cómo y cuándo debe despedirse o sustituirse a un DPD por otra persona. No obstante, cuanto más estable sea el contrato de un DPD, y más garantías existan contra el despido improcedente, tendrán más posibilidad de actuar con independencia. Por consiguiente, el GP29 acogería con beneplácito los esfuerzos de las organizaciones en ese sentido.

3.5. Conflicto de interés

El artículo 38(6) permite a los DPD «desempeñar otras tareas y funciones». No obstante, exige que la organización garantice que «tales tareas y funciones no deriven en un conflicto de interés».

La ausencia de conflicto de interés está estrechamente ligada al requisito de actuar con independencia. Aunque se permite a los DPD tener otras funciones, solo se les puede confiar otras tareas y funciones siempre que estas no originen conflictos de interés. Esto supone en especial que el DPD no puede detentar un cargo dentro de 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[34].

[34] Por regla general, los cargos en conflicto pueden incluir los puestos de alta dirección (tales como director ejecutivo, director de operaciones, director economicofinanciero, director médico, jefe del departamento de marketing, director de recursos humanos o jefe del departamento de TI), pero también otros puestos inferiores en la estructura organizativa si tales cargos o funciones llevan a la determinación de los fines y medios del tratamiento.

Dependiendo de las actividades, el tamaño y la estructura de la organización, puede ser recomendable para los responsables o encargados del tratamiento:

- determinar qué puestos serían incompatibles con la función de DPD
- redactar normas internas a estos efectos para evitar conflictos de interés
- incluir una explicación más general sobre los conflictos de interés
- declarar que su DPD no tiene ningún conflicto de interés en relación con su función como DPD, como medio de concienciar sobre este requisito
- incluir salvaguardas en las normas internas de la organización y garantizar que el anuncio de vacante para el puesto de DPD o el contrato de servicios sea lo suficientemente preciso y detallado para evitar un conflicto de interés. En este contexto, debe tenerse en cuenta que los conflictos de interés pueden adoptar diversas formas en función de si el DPD se contrata interna o externamente.

4 Funciones del DPD

4.1. Control del cumplimiento de la NGPD

El artículo 39(1)(b) encomienda a los DPD, entre otras funciones, la de controlar el cumplimiento de la NGPD. El considerando 97 especifica además que el DPD «debe ayudar al responsable o el encargado del tratamiento a controlar el cumplimiento interno del presente Reglamento».

Como parte de estas funciones de control del cumplimiento, los DPD pueden, en particular:

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

El control del cumplimiento no significa que el DPD sea responsable personalmente en caso de algún incumplimiento. La NGPD declara taxativamente que es el responsable del tratamiento, no el DPD, quien está obligado a «implementar las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento se lleva a cabo con arreglo al presente Reglamento» (artículo 24(1)). El cumplimiento de la normativa de protección de datos es una responsabilidad corporativa del responsable del tratamiento, no del DPD.

4.2. El papel del DPD en una evaluación de impacto de la protección de datos

Según el artículo 35(1), es tarea del responsable del tratamiento, no del DPD, llevar a cabo, cuando sea preciso, una evaluación de impacto de la protección 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 por diseño, el artículo 35(2) establece específicamente que el responsable del tratamiento «deberá solicitar asesoramiento» al DPD cuando lleve a cabo una evaluación de impacto de la protección de datos. El artículo 39(1)(c), a su vez, encomienda al DPD la tarea de «ofrecer asesoramiento cuando se solicite en relación con la evaluación de impacto de la protección de datos y controlar su ejecución».

El GP29 recomienda que el responsable del tratamiento solicite el asesoramiento del DPD sobre las siguientes cuestiones, entre otras[35]:

- si se debe llevar a cabo o no una evaluación de impacto de la protección de datos
- qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos
- si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa
- qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados
- si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con la NGPD.

Si el responsable del tratamiento está en desacuerdo con el consejo expresado por el DPD, la documentación de la evaluación de impacto de la protección de datos deberá justificar específicamente por escrito por qué el consejo no se ha tenido en cuenta[36].

El GP29 recomienda además que el responsable del tratamiento describa, por ejemplo en el contrato de DPD, pero también en la información proporcionada a los empleados, a la dirección (y a otras partes interesadas, cuando proceda), las tareas exactas del DPD y su alcance, en especial por lo que se refiere a la realización de la evaluación de impacto de la protección de datos.

4.3. Enfoque basado en el riesgo

El artículo 39(2) establece que el DPD deberá «considerar debidamente el riesgo asociado a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento».

Este 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 prioricen sus actividades y centren sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos. Esto no significa que deban descuidar el control de la conformidad de las operaciones de tratamiento de datos que comparativamente presenten un menor nivel de riesgo, sino que deben centrarse primordialmente en las áreas de mayor riesgo.

Este enfoque selectivo y pragmático debe ayudar a los DPD a asesorar al responsable del tratamiento sobre qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos, qué áreas deben someterse a auditoría de protección de datos interna o externa, qué actividades de formación internas proporcionar al personal o los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

[35] El artículo 39(1) menciona las tareas del DPD e indica que el DPD tendrá «al menos» las siguientes tareas. Por lo tanto, nada impide al responsable del tratamiento asignar al DPD otras tareas aparte de las mencionadas expresamente en el artículo 39(1) o especificar dichas tareas con más detalle.

[36] El artículo 24(1) estipula que «teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad que afectan a los derechos y libertades de las personas físicas, el responsable del tratamiento deberá implementar medidas técnicas y organizativas apropiadas para garantizar **y poder demostrar** que el tratamiento se lleva a cabo de acuerdo con el presente Reglamento. Dichas medidas se revisarán y se actualizarán cuando sea necesario».

4.4. El papel del DPD en el mantenimiento de los registros

Según el artículo 30, apartados 1 y 2, es el responsable o el encargado del tratamiento, no el DPD, quien está obligado a «mantener un registro de las operaciones de tratamiento de las que es responsable» o a «mantener un registro de todas las categorías de actividades de tratamiento llevadas a cabo en nombre de un responsable del tratamiento».

En la práctica, los DPD suelen elaborar inventarios y mantener un registro de las operaciones de tratamiento basados en la información que les proporcionan los diversos departamentos de su organización responsables del tratamiento de datos personales. Esta práctica se ha instaurado de acuerdo con muchas leyes nacionales en vigor y conforme a las normas sobre protección de datos aplicables a las instituciones y los organismos de la UE[37].

El artículo 39(1) señala una lista de cometidos que el DPD debe tener como mínimo. Así pues, nada impide al responsable del tratamiento o al encargado asignar al DPD la tarea de mantener el registro de las operaciones de tratamiento que son responsabilidad del responsable del tratamiento. Dicho registro debe considerarse una de las herramientas que permiten al DPD llevar a cabo sus funciones de control del cumplimiento, información y asesoramiento al responsable o el encargado del tratamiento.

En cualquier caso, el registro que se requiere mantener según el artículo 30 debe verse también como una herramienta que permite al responsable del tratamiento y a la autoridad supervisora, cuando así se solicite, tener una perspectiva general de todas las actividades de tratamiento de datos personales que lleva a cabo una organización. Es por lo tanto un requisito previo para el cumplimiento de la normativa y, en ese sentido, una medida de rendición de cuentas efectiva.

[37] Artículo 24(1)(d), Reglamento (CE) 45/2001.