

En el escrito de consulta se plantean diversas cuestiones relativas a la figura del delegado de protección de datos (**DPD**), incorporada a nuestro ordenamiento jurídico en virtud de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE.

Por la asociación consultante se interesa el criterio de este Gabinete Jurídico sobre determinadas cuestiones vinculadas al nombramiento de los delegados de protección de datos -DPD- y al desempeño de sus funciones en el ámbito de las entidades a las que se refiere su designación, refiriéndose a la necesidad del cumplimiento de los requisitos formales y materiales establecidos por la normativa aplicable, especialmente en lo relativo a su grado de profesionalización e independencia.

I

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos -**RGPD**-), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales -**LOPDGDD**- conforman el marco jurídico de referencia en España que afecta a la protección de datos de carácter personal.

En estas normas se regulan los principios y fundamentos a los que deben ajustarse la recogida y tratamiento de los datos personales por cualquier persona pública o privada que lleve a cabo tratamiento de datos de carácter personal en el ejercicio de su actividad, sin perjuicio de las normas especiales existentes para determinadas actividades o tratamientos, como por ejemplo los tratamientos de datos personales sujetos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Como ha señalado reiteradamente esta Agencia y se recoge en la Exposición de motivos de la LOPDGDD, “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”.

Un papel fundamental dentro del nuevo modelo de responsabilidad activa lo desempeñará el delegado de protección de datos. Siguiendo también en este punto la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, “la figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.”

La labor divulgativa y de *sensibilización que* -de acuerdo con los artículos 57 y 58 del RGPD, y el artículo 47 de la LOPDGDD-, *corresponde a la* Agencia Española de Protección de Datos, se ha plasmado en la publicación de diversos documentos, herramientas y guías prácticas en las que se aborda, entre otras cuestiones, el papel del delegado de protección de datos, así como los requisitos para su designación.

Así, por ejemplo, en la “Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento (<https://www.aepd.es/sites/default/files/2019-12/guia-rgpd-para-responsables-de-tratamiento.pdf>)”, en el documento sobre “Novedades de la LOPDGDD para el sector privado (<https://www.aepd.es/sites/default/files/2019-10/novedades-lopd-sector-privado.pdf>)”, en el documento sobre “Novedades de la LOPDGDD para los ciudadanos (<https://www.aepd.es/sites/default/files/2019-10/novedades-lopd-ciudadanos.pdf>)”, en la “Guía sobre Protección de Datos y Administración Local (<https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf>)” y, más recientemente, en el documento informativo

sobre “Adecuación a la normativa coste cero y otras prácticas fraudulentas (<https://www.aepd.es/sites/default/files/2019-09/coste-cero.pdf>).

De tal modo, en orden a la promoción de la necesaria “sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben” -*ex artículo 57.1 d) RGPD*-, los referidos documentos informativos, así como otros muchos publicados en el canal web de la Agencia -www.aepd.es-, vienen prestando especial atención a la figura del delegado de protección de datos, a su regulación y a las consecuencias prácticas que deriva de esta figura en relación con las organizaciones públicas y privadas que vienen obligadas a su designación.

Asimismo, la Agencia viene incorporando un extenso material orientativo y formativo en torno a la figura del delegado de protección de datos, cuya consulta pública puede realizarse en el siguiente enlace: <https://www.aepd.es/es/guias-y-herramientas/herramientas/canalDPD>.

La Sección 4 del CAPÍTULO IV, del RGPD -artículos 37 a 39-, regula de forma detallada la figura del delegado de protección de datos. En relación con la interpretación y aplicación de estos preceptos puede acudir a las pautas contenidas en el documento del Grupo del Artículo 29 “Directrices sobre los Delegados de Protección de Datos” -WP243-, revisadas por última vez y adoptadas el 5 de abril de 2017 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048).

A su vez, recientemente, como parte del proyecto “T4Data - Formación para Protección de Datos”, *financiado por la Unión Europea*, se ha elaborado un manual práctico sobre el DPD (Delegado de Protección de Datos) -“*Guía para los Delegados de Protección de Datos en los sectores públicos y semipúblicos sobre cómo garantizar el cumplimiento del Reglamento General de Protección de Datos de la Unión Europea (Reglamento (UE) 2016/679)*”-.

La información y las opiniones expuestas en dicho manual son las de sus autores, y no reflejan necesariamente la opinión oficial de la Unión Europea. Ni las instituciones y organismos de la Unión Europea, ni ninguna persona que actúe en su nombre podrá ser considerada responsable del uso que pueda hacerse de la información que contiene dicho manual.

Esta guía orientativa puede obtenerse en el siguiente enlace: <https://www.aepd.es/sites/default/files/2019-12/EI%20Manual%20del%20DPD%20-%20KORFFGEORGES%20-%20ESP.pdf>.

El manual ha sido preparado como parte de los materiales para el programa de formación de formadores “T4DATA” financiado por la UE, destinado a formar al personal de varias agencias de protección de datos (APD) de los Estados miembros de la UE en la formación de delegados de protección de datos (DPD), especialmente en el sector público, en sus nuevas

obligaciones bajo el Reglamento General de Protección de Datos. El proyecto se lleva a cabo bajo la iniciativa de la Agencia Italiana de Protección de Datos, “*La Garante per la protezione dei dati personali*”, y es administrado por la “*Fondazione Basso*”, con la ayuda de dos expertos del Grupo de Expertos en Derechos Fundamentales de Europa (FREE). Esta guía está basada en contribuciones importantes del “Garante” y de otros socios europeos que enviaron ejemplos prácticos muy útiles y copias de sus propias notas de orientación sobre el RGPD.

La participación de la Agencia Española de Protección de Datos en esta “Guía para los Delegados de Protección de Datos”, se plasma, muy especialmente, en la introducción de instrumentos de certificación en relación con la formación y acreditación de los delegados de protección de datos, a los que se hace mención en el manual.

Este sistema de certificación formal para delegados se encuentra ya plenamente operativo, resultando previsible, según se señala en el propio documento que, “en el futuro, aparte de España, otros Estados miembros también proporcionen dichos esquemas formales, oficialmente reconocidos, y/o el Consejo Europeo de Protección de Datos pueda (probablemente de manera informal) respaldar algunos.”

En efecto, esta Agencia ha establecido un *Esquema de Certificación* de Delegados de Protección de Datos (Esquema AEPD-DPD) bajo el cual la Entidad Nacional de Acreditación -ENAC- puede acreditar a Entidades de Certificación que a su vez estarán autorizadas a emitir una certificación relevante sobre la base de criterios desarrollados por la AEPD y un examen formal.

Dicho *Esquema* incorpora un sistema de certificación que permite certificar que los DPD reúnen la cualificación profesional y los conocimientos requeridos para ejercer la profesión. Las certificaciones son otorgadas por entidades certificadoras debidamente acreditadas por ENAC. El sistema puede consultarse en <https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos/certificacion>.

Así, aunque esta certificación *no es obligatoria* para poder ejercer como delegado de protección de datos, y se puede ejercer la profesión sin estar certificado bajo éste o cualquier otro esquema, la Agencia ha considerado necesario ofrecer un punto de referencia al mercado sobre los contenidos y elementos de un mecanismo de certificación que pueda servir como garantía para acreditar la cualificación y capacidad profesional de los candidatos a DPD.

El documento que contiene el “Esquema de certificación de delegados de protección de datos de la Agencia Española de Protección de Datos

(ESQUEMA AEPD-DPD)” puede consultarse en el siguiente enlace <https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf>.

De otra parte, este Gabinete Jurídico ha tenido ocasión de abordar en numerosas ocasiones el análisis de la figura del delegado de protección de datos. Así, entre otros, (i) en nuestro Informe 0011/2019 se contiene el criterio de esta Agencia referido a determinadas cuestiones vinculadas al nombramiento del DPD en el ámbito de la Administración pública, (ii) en nuestro Informe 0100/2019, sobre la obligatoria designación de más de un delegado de protección de datos en el ámbito de un determinado Ministerio, se analiza la procedencia de la designación de uno o más delegados para los supuestos planteados, (iii) en el Informe 0167/2018 se examina la compatibilidad funcional del delegado de protección de datos del RGPD y el responsable de seguridad del Esquema Nacional de Seguridad, y (iv) en el Informe 0170/2018 se abordan cuestiones sustantivas referidas a la diferenciación entre seguridad de información y protección de datos de carácter personal, y su incidencia en la labor del delegado de protección de datos.

Finalmente, -por todos- en los Informes 0133/2019 y 0148/2019, partiendo del principio de responsabilidad proactiva, se señala que sólo en el caso de que el delegado de protección de datos tenga dudas jurídicas sobre el asunto sometido a su consideración -que no puedan resolverse con los criterios ya informados por la AEPD- o por tratarse de cuestiones nuevas derivadas de la aplicación del nuevo régimen jurídico de protección de datos de carácter personal y que tengan un alcance general en el que resulte conveniente un informe que contribuya a la seguridad jurídica, podrá elevar consulta a este Gabinete Jurídico, acompañando a dicha consulta su propio informe en el que se analicen detallada y motivadamente las cuestiones planteadas.

II

En primer lugar, por la asociación consultante se interesa la opinión de este Gabinete Jurídico respecto de los criterios para la designación del DPD, con referencia a la preparación teórica y práctica necesaria para su correcta designación, y con especial mención de la necesidad de que existan profesionales DPD tras la designación de entidades jurídicas como DPD.

Según se expone en la consulta, en ocasiones, (i) las entidades especializadas que ofrecen servicios en materia de protección de datos vienen prestando funciones de DPD sin proceder formalmente a su nombramiento, mientras que, en otros supuestos, (ii) se procede a la designación de ciertas entidades como DPD, no contando en su organización con profesionales con la preparación necesaria para cumplir con sus cometidos, (iii) el nombramiento del DPD se refiere a un número de clientes tan excesivo que es muy probable que no puedan atender sus funciones con la debida solvencia profesional, o (iv) el nombramiento del DPD carecería de validez al incumplirse los criterios exigidos para su designación.

La Sección 4 del CAPÍTULO IV, del RGPD -artículos 37 a 39-, regula de forma detallada la figura del delegado de protección de datos. Esta regulación se ve complementada con lo dispuesto en el CAPÍTULO III del TÍTULO V de la LOPDGDD-, en cuyos *artículos 34 a 37* se contienen algunas especialidades directamente aplicables a nuestro derecho interno.

En concreto, la designación del delegado de protección de datos se recoge en el artículo 37 del RGPD, *ampliándose* en el artículo 34 de la LOPDGDD el espectro de sujetos obligados a su nombramiento.

En particular, el artículo 37.1 a) impone obligatoriamente la designación de un delegado en los supuestos en que el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial, contemplándose también su nombramiento atendiendo al *tipo de actividades* que lleve a cabo el responsable (o encargado), cuando - *artículo 37.1 b)*- las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o/y cuando -*artículo 37.1 c)*- las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Este precepto se complementa con lo dispuesto en el artículo 34.1 de la LOPDGDD, que especifica determinados supuestos en los que resulta obligatoria la designación de un DPD. De la regulación contenida en este artículo se extrae la obligatoriedad de la designación de un DPD en relación con la *multiplicidad de tratamientos* de datos a los que se refiere, respondiendo así a las exigencias derivadas de la naturaleza y características de dichos tratamientos, que imponen la necesidad del nombramiento del delegado en orden a la mejor garantía del *cumplimiento proactivo* de la normativa de protección de datos.

Como queda expuesto, en todos los supuestos de los artículos 37 del RGPD y 34 de la LOPDGDD, deberá procederse a la designación de DPD.

III

De lo anterior se extrae que la exigencia del nombramiento de DPD no debe interpretarse, sin más, como una mera formalidad, debiendo cumplirse con los requisitos establecidos en las normas jurídicas aplicables.

En consecuencia, resulta necesario realizar un somero análisis de las *funciones y recursos* de los que deberá disponer el DPD.

Así, para la adecuada resolución de las cuestiones planteadas, debe partirse de las importantes *funciones* que el artículo 39.1 del RGPD asigna al DPD:

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

- a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
- c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
- d) cooperar con la autoridad de control;
- e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.”

Se trata, por consiguiente, de funciones de asesoramiento y supervisión dirigidas a garantizar el adecuado cumplimiento de la normativa sobre protección de datos personales, señalando el artículo 39.2 que “El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento”. Asimismo, el artículo 38.1 establece claramente que “El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe *de forma adecuada y en tiempo oportuno* en todas las cuestiones relativas a la protección de datos personales”.

Además de las importantes funciones de asesoramiento que el DPD tiene asignadas, incluidos los supuestos en los que sea necesario realizar una evaluación de impacto por tratarse de tratamientos de alto riesgo, y precisando las funciones de supervisión, el artículo 36 de la LOPDGDD prevé que “El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias”, que “En el ejercicio de sus funciones el delegado de protección

de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica” y que “Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento”.

Asimismo, en cuanto a las relaciones con esta Agencia, debe tenerse en cuenta que corresponde al DPD, conforme al artículo 39.1.d) del RGPD, cooperar con la autoridad de control, siendo destacable a estos efectos la regulación que el artículo 37 de la LOPDGDD realiza de la intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos:

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

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

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

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

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

Por otro lado, el artículo 39.1.e) del RGPD establece también como funciones del DPD “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”. Precisamente, atendiendo al nuevo modelo establecido en el RGPD y a las funciones encomendadas al DPD en cuanto al asesoramiento al responsable y a la realización de consultas a la AEPD, es criterio reiterado de este Gabinete Jurídico que “si el responsable del tratamiento tiene dudas sobre

la base jurídica que pueda determinar la licitud de un determinado tratamiento deberá consultar a su delegado de protección de datos en los supuestos en que, como el presente, su designación es obligatoria, quien deberá prestarle el asesoramiento preciso. Sólo en el caso de que el delegado de protección de datos tuviera dudas jurídicas sobre el asunto sometido a su consideración que no puedan resolverse con los criterios ya informados por la AEPD o por tratarse de cuestiones nuevas derivadas de la aplicación del nuevo régimen jurídico de protección de datos de carácter personal y que tengan un alcance general en el que resulte conveniente un informe que contribuya a la seguridad jurídica, podrá elevar dicho delegado consulta a este Gabinete Jurídico, acompañando a dicha consulta su propio informe en el que se analicen detallada y motivadamente las cuestiones objeto de consulta”. Así lo ha venido exponiendo esta Agencia en diferentes informes jurídicos, por todos, el **148/2019**, 24 de noviembre de 2020.

Para el adecuado cumplimiento de dichos cometidos, el RGPD exige unos requisitos de *capacitación* del DPD, y que al mismo se le dote de los *recursos necesarios*.

A los requisitos de capacitación, se refiere el artículo 37.5 RGPD, disponiendo 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”.

Por su parte, el artículo 35 de la LOPDGDD añade que “El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en derecho y la práctica en materia de protección de datos”.

En orden a la mejor interpretación y aplicación de estos preceptos, puede acudir a las pautas contenidas en el documento del Grupo del Artículo 29 “Directrices sobre los Delegados de Protección de Datos” -WP243-, revisadas por última vez y adoptadas el 5 de abril de 2017, que, en relación con los conocimientos y habilidades del DPD, señalan los siguientes puntos:

- *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 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, los derechos de los interesados, la protección de los datos desde el diseño y por defecto, el registro de las actividades de tratamiento, la seguridad del tratamiento y la notificación y comunicación de las violaciones de la seguridad de los datos.

Por otro lado, la necesidad de dotar al DPD de los *recursos necesarios* para el desempeño de sus funciones se recoge como una obligación del responsable en el artículo 38.2 del RGPD: “El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados”.

A este respecto, en las Directrices del Grupo del 29 se indica lo siguiente:

“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 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.”

Como consecuencia de su carácter y naturaleza jurídica, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *tiene efecto directo y se aplica directamente* en los Estados Miembro sin necesidad de que éstos adopten ninguna norma de introducción en el derecho interno. Dicho carácter y eficacia directa se cohonesta de manera pacífica con las exigencias derivadas del principio de legalidad y seguridad jurídica recogidos en la Constitución Española y en la normativa sobre procedimiento administrativo común.

Por otra parte, según se ha expuesto anteriormente, las Directrices del Grupo del 29, se refieren *tanto* a la necesidad de que el DPD disponga del tiempo suficiente para el cumplimiento de sus funciones, *como* a la estrecha relación entre las funciones del DPD y el tamaño y estructura de las organizaciones en las que se desarrolla su actividad (apartado 2.3.de las Directrices).

En definitiva, el nombramiento de un determinado DPD que desempeñe sus servicios en relación con una multiplicidad de responsables y/o encargados del tratamiento, *es una decisión del responsable* que se considera admisible siempre que se cumpla con los requisitos de capacitación, suficiencia de medios, disponibilidad e independencia que establece el RGPD, y que se garantice que dicho DPD participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales, atendiendo a los requisitos de suficiencia de medios.

Por consiguiente, tal y como señalábamos en nuestro *Informe 100/2019*, de 11 de febrero de 2020, **lo esencial no es el número de DPD, ni siquiera que estos formen parte de la organización del responsable** (el apartado 6 del artículo 37 prevé que “el delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios”) **sino que lo relevante es que los mismos reúnan los requisitos de capacitación e independencia que les permitan desarrollar adecuadamente las funciones que el RGPD les asigna**, teniendo en cuenta que, como recuerda el Considerando 97 del RGPD, “El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o encargado”.

De este modo, siendo la designación de DPD por una entidad pública o privada una cuestión eminentemente organizativa, y siempre que quede adecuadamente garantizada su independencia, **lo relevante es que las funciones que se asignan al DPD se puedan realizar con eficacia, debiendo tenerse en cuenta, igualmente, el criterio de la disponibilidad, fundamental para garantizar que los interesados puedan fácilmente contactar con el DPD** (conforme al artículo 38.4 del RGPD, “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”).

En conclusión, dichas funciones podrán desarrollarse eficazmente si se cumple con los requisitos de capacitación al proceder a la designación del DPD y se le dota de los recursos necesarios, incluido, como señala el Grupo del Artículo 29 un equipo de DPD (un DPD y su personal), equipo que deberá ser proporcional al tamaño y estructura de la organización, así como a la sensibilidad, complejidad y cantidad de los datos que una organización trata, debiendo garantizarse la disponibilidad del DPD de modo que los interesados puedan contactar con él, así como comunicarse con las autoridades de protección de datos.

IV

En segundo lugar, la consulta plantea la validez legal del nombramiento del DPD realizado mediante designación en favor de personas vinculadas a la propia organización, que, según la consultante, podría poner en duda la *independencia* del delegado y derivar en posibles *incompatibilidades* en el desarrollo de su actividad.

En este punto, antes de abordar las cuestiones relativas a la *independencia* y los *posibles conflictos de intereses* del delegado, debe insistirse en la clara diferenciación, de una parte, entre la figura del responsable del tratamiento y la del delegado de protección de datos, y, de otra parte, entre la figura del delegado y la del responsable de seguridad.

En relación con *la primera de las distinciones*, el RGPD es claro a la hora de imponer al responsable del tratamiento la obligación de cumplimiento de las medidas que el mismo prevé. Será así el responsable quien deba mantener un registro de operaciones de tratamiento, evaluar el riesgo concurrente en un determinado tratamiento de datos o desarrollar en su caso a evaluación de impacto exigida por el reglamento. Del mismo modo, será el que habrá de determinar las medidas técnicas y organizativas que hayan de adoptarse para garantizar la seguridad del tratamiento. Lógicamente, estas medidas se desarrollarán por quienes las tuvieran atribuidas dentro de la estructura del responsable, siendo especialmente relevantes a estos efectos los distintos sujetos que participen activamente en la implantación de las medidas de seguridad de la información y, particularmente, el responsable de seguridad.

Frente a lo que acaba de indicarse, la función del delegado de protección de datos será la de prestar al responsable la asistencia y asesoramiento necesarios en el proceso de adopción de las medidas y supervisar que las mismas se han adoptado y se llevan a la práctica. Es decir, el delegado de protección de datos asesora al responsable y controla el

cumplimiento de las obligaciones establecidas por la normativa de protección de datos de carácter personal.

En este sentido, el documento de directrices WP243, adoptado por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, señala que “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”.

Asimismo, tal y como señalábamos en nuestro Informe 170/2018, de 12 de noviembre de 2018, es importante *diferenciar* claramente la designación y funciones del delegado de protección de datos de las del *responsable de seguridad* de las organizaciones públicas o privadas. En dicho Informe se señalaba la clara diferenciación entre el DPD y el responsable de seguridad del Esquema Nacional de Seguridad -ENS-, de modo que:

“IV

Las posiciones del RSEG y del DPD son requisitos exigidos en normas diferenciadas con objetivos y ámbitos de aplicación distintos y, el principio de independencia del DPD, debería entenderse de manera amplia incluso con relación a las figuras que menciona el artículo 10 del ENS. En el mismo orden de ideas, cabría tener en cuenta que el propio principio de segregación de funciones del ENS tuviera en cuenta la separación de los roles indicados (RINF, RSEG, RSER) con relación a las funciones del DPD.

Debe entenderse que la función de seguridad de la información es una herramienta que permite abordar el cumplimiento de lo previsto en el artículo 32 del RGPD, pero no puede entenderse como una herramienta que garantice el pleno e íntegro cumplimiento del RGPD. En consecuencia, las funciones del RSEG tienen un alcance limitado en el RGPD frente al alcance de las competencias del DPD.

Carece de sentido que se especifique la diferenciación de los tres roles relacionados con la seguridad de la información en las Administraciones Públicas, y se quiera asignar ahora un rol adicional, el de DPD, al responsable de seguridad de la información. Resulta claro que un DPD, alimentará de requisitos, aconsejará y supervisará a los tres responsables: información, servicio y seguridad. Si el responsable de seguridad asume las tareas de DPD, se le asigna de forma directa tareas de los otros dos responsables, lo que contradice el propio ENS y, sin duda, generaría posibles conflictos de intereses que podrían afectar a los derechos y libertades de las personas o incluso a la propia seguridad de la información.

En definitiva, esa diferenciación de tareas que garantiza la efectividad del trabajo del responsable de seguridad tiene sentido extenderla a que no se le asignen tareas no específicas de su función. Del mismo modo que la necesaria

independencia del DPD y la necesidad de evitar los conflictos de intereses impide asignarle responsabilidades directas en un ámbito que va a tener que supervisar y en el que estará sujeto a instrucciones de otros órganos.

Así lo han entendido en organizaciones con importantes responsabilidades en materia de seguridad de la información. (...)

V

En conclusión, es criterio de este Gabinete Jurídico que, con carácter general, debe existir la necesaria separación entre el delegado de protección de datos regulado en el RGPD y el responsable de seguridad del ENS, sin que sus funciones puedan recaer en la misma persona u órgano colegiado.

Solo excepcionalmente, en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar dicha separación, sería admisible la designación como delegado de protección de datos de la persona que ejerciera las funciones de responsable de seguridad del ENS, siempre que en la misma concurren los requisitos de formación y capacitación previstos en el RGPD. Además, resultaría imprescindible adoptar todas las medidas organizativas, debidamente reflejadas en su Política de seguridad de la información, que garantice la necesaria independencia y la ausencia de conflicto de intereses, por lo que no podría recibir instrucciones respecto al desempeño de sus funciones como delegado de protección de datos, deberá responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. En todo caso, esta circunstancia, que como decíamos, tiene carácter excepcional, deberá evaluarse caso por caso, y deberá dejarse documentada dicha designación haciendo constar los motivos por lo que el organismo correspondiente no ha podido observar dicha separación de funciones, así como las medidas que garantizan *la necesaria independencia* del delegado de protección de datos.”

Una vez realizadas las anteriores acotaciones, y respondiendo ya a las cuestiones planteadas -relativas a la *independencia* del DPD y a las posibles *incompatibilidades* en el ejercicio de su actividad-, deberá estarse a las normas jurídicas que la regulan la posición del delegado en sus relaciones con el responsable y/o con el encargado del tratamiento.

Así, el artículo 36 de la LOPDDD, dispone lo siguiente:

“Posición del delegado de protección de datos”

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.
2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, **el delegado de protección de datos no podrá ser**

removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.” (la negrita es nuestra)

Por su parte, el artículo 38.3 del RGPD, al regular la posición del delegado de Protección de Datos, subraya su *independencia* al señalar que el responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones, *no pudiendo ser destituido ni sancionado* por el responsable o el encargado por desempeñar sus funciones, y rindiendo cuentas directamente al más alto nivel jerárquico del responsable o encargado.

Además, según el documento del Grupo del Artículo 29 “Directrices sobre los Delegados de Protección de Datos”, revisadas por última vez y adoptadas el 5 de abril de 2017 -WP243-, en su nombramiento debe tenerse en consideración el elemento relativo a la *independencia* del DPD, de modo que:

Independencia: El artículo 38.3 del Reglamento establece unas garantías básicas para que los delegados actúen con independencia dentro de la organización en la que prestan sus servicios, incluyendo que “no reciban ninguna instrucción relativa al ejercicio de sus tareas”. Además, es importante señalar que los obligados al cumplimiento del RGPD son el responsable o el encargado del tratamiento, de forma que, si adoptan decisiones contrarias a la norma y al asesoramiento prestado por el delegado, debe darse a este la posibilidad de expresar con claridad su opinión disconforme respecto a dichas decisiones.

Destitución: El anteriormente citado artículo 38.3 también se refiere a que los delegados de protección de datos “no deben ser destituidos ni penalizados por el responsable o el encargado por llevar a cabo sus funciones”, lo que supone un *refuerzo de su autonomía e independencia*. Sí podría ser despedido o sancionado de conformidad con la legislación contractual, laboral o penal aplicable de cada país, por causas distintas al desempeño de sus funciones. Téngase en cuenta en el ámbito de las Administraciones públicas el régimen de infracciones y sanciones aplicables a su personal.”

En relación con el posible conflicto de intereses del delegado, las directrices sobre los delegados de protección de datos adoptadas por el Grupo de Trabajo sobre Protección de Datos del Artículo 29, revisadas por última vez y adoptadas el 5 de abril de 2017 -WP243-, señalan lo siguiente:

“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."

De lo anterior se extrae que, **al margen de la fórmula adoptada para su nombramiento, la designación del delegado de protección de datos ha de responder a las exigencias derivadas del principio de independencia en el desarrollo de su actividad, debiendo garantizarse que el desempeño de sus funciones y cometidos no den lugar a conflicto de intereses.**

La provisión de delegado de protección de datos en las organizaciones públicas o privadas exige que la selección se ajuste a los requisitos legalmente establecidos y, en especial, que se acrediten los conocimientos especializados en derecho y práctica de la protección de datos que señala el RGPD. Por lo demás, la fórmula adoptada para el nombramiento de DPD dependerá de la decisión adoptada por la entidad en la que desempeñe sus funciones, como consecuencia de su *autonomía organizativa*.

Sin embargo, las cuestiones relativas a la autonomía de las organizaciones en las que se encuadren los delegados, claramente derivadas en la normativa analizada en este informe, no pueden ser óbice para la necesaria *garantía de la independencia del delegado de protección de datos - ex artículo 38 RGPD-* en el marco de las relaciones jurídicas internas y externas que mantenga en el desarrollo de sus funciones.

Así, en todo caso, resultará exigible, tal y como prevé el artículo 36 de la LOPDGDD, que (i) cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos *no pueda ser removido ni sancionado* por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio, que (ii) *se garantice la independencia* del delegado de protección de datos dentro de la organización, debiendo evitarse

cualquier conflicto de intereses, y que (iii) cuando el delegado de protección de datos aprecie la existencia de *una vulneración relevante en materia de protección de datos lo documente y comunique* inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

En definitiva, *si bien* la Sección 4 del CAPÍTULO IV, del RGPD -artículos 37 a 39-, contempla para los DPD amplias posibilidades en cuanto a su nombramiento y encuadre en la organización de las entidades a las que se refiere su designación, no es menos cierto que **dicha autonomía debe conciliarse con las exigencias derivadas del principio de independencia del delegado, debiendo garantizarse que el ejercicio de sus funciones no dé lugar situaciones de incompatibilidad, ni a conflicto de intereses.**

En las normas jurídicas que regulan la figura del delegado de protección de datos, se configuran el requisito de su independencia como consustancial al desempeño de sus funciones.

V

Una vez expuesto someramente el régimen jurídico del DPD, procede ahora aludir al régimen sancionador del Título V de la Ley Orgánica 3/2018, de 5 de diciembre, en el que, después de señalar en su artículo 71 que “Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica”, se identifican a efectos de prescripción el elenco de infracciones de responsables y encargados de los tratamientos, así como las consecuencias jurídicas derivadas de un eventual incumplimiento. En particular, de acuerdo con sus artículos 73 y 74:

“Artículo 73. Infracciones consideradas graves.

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

(...)

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

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

(...)”

“Artículo 74. Infracciones consideradas leves.

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

(...)

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

En cuanto a las consecuencias jurídicas derivadas de estas infracciones, el *artículo 76* de la LOPDGDD remite a las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del RGPD, que deben aplicarse teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo, sin perjuicio del régimen aplicable a determinadas categorías de responsables o encargados del tratamiento, señalados en el *artículo 77* de la propia Ley Orgánica 3/2018, de 5 de diciembre.

A su vez, la Disposición adicional decimosexta de la LOPDGDD, referida a prácticas agresivas en materia de protección de datos, dispone que, a los efectos previstos en el artículo 8 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, se considera como práctica agresiva (entre otras) la señalada en su *letra e*), consistente en “asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos.”

En materia sancionadora, las exigencias derivadas de los principios de legalidad y tipicidad, proclamados por la Constitución Española, se contemplan en diferentes artículos de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. En este sentido, destaca la regulación de su artículo 25, relativa al principio de legalidad, que exige que la potestad sancionadora de las Administraciones públicas se ejerza sólo cuando haya sido expresamente reconocida por una norma con rango de Ley, correspondiendo su ejercicio únicamente a los órganos administrativos que la tengan expresamente atribuida.

A su vez, de acuerdo con el principio de tipicidad recogido en el artículo 27 de la misma norma, *(i)* sólo constituyen infracciones administrativas las vulneraciones del ordenamiento jurídico previstas como tales infracciones por una Ley (...), *(ii)* únicamente por la comisión de infracciones administrativas podrán imponerse sanciones que, en todo caso, estarán delimitadas por la Ley, *(iii)* las disposiciones reglamentarias de desarrollo podrán introducir especificaciones o graduaciones al cuadro de las infracciones o sanciones establecidas legalmente que, sin constituir nuevas infracciones o sanciones, ni alterar la naturaleza o límites de las que la Ley contempla, contribuyan a la más correcta identificación de las conductas o a la más precisa determinación de las

sanciones correspondientes, y (iv) las normas definidoras de infracciones y sanciones no serán susceptibles de aplicación analógica.

Así, en relación con la obligatoria designación de delegado de protección de datos, la Agencia ha dictado diversas resoluciones sancionadoras, por todas, en lo relativo Administraciones públicas, la dictada en el marco del procedimiento sancionador PS/00001/2020, dirigida contra un ayuntamiento por la infracción del artículo 37 del RGPD, al carecer este de DPD, y, en el ámbito privado, la recaída en el expediente sancionador PS/00417/2019, seguido contra una entidad privada también por carecer de dicho Delegado, que ha llevado aparejada la imposición de una sanción de 25.000 euros a dicha entidad, también por una infracción del artículo 37 del RGPD.

Para concluir, y sin perjuicio de las infracciones específicas relacionadas con el DPD anteriormente citadas, hay que resaltar que, en la práctica, el delegado de protección de datos asume principalmente funciones de asesoramiento y supervisión en beneficio del responsable o encargado. Sin embargo, como señala claramente el RGPD en diferentes preceptos, el responsable tendrá responsabilidad plena ante la ley por cualquier fallo en ese sentido, sin que, en ningún caso, dicha responsabilidad recaiga sobre el DPD.

Concretamente, tal y como dispone el artículo 5.2 del RGPD, “El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)", y es al responsable al que le corresponde aplicar “medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento” (artículo 24.1. del RGPD)

En otras palabras, esa responsabilidad no descansa sobre el DPD, como también se desprende del artículo 39 del RGPD -que enfatiza sus tareas de asesoramiento y apoyo-, sino en el propio responsable, o, en su caso, en el encargado del tratamiento. En consecuencia, los responsables y los encargados de los tratamientos serán los principales interesados en velar por el cumplimiento de los requisitos exigidos para la correcta designación del DPD y por facilitarle el ejercicio de sus funciones ya que, en otro caso, serán los que respondan ante un eventual incumplimiento de las obligaciones impuestas por la normativa de protección de datos.

En este sentido, en las “Directrices sobre los Delegados de Protección de Datos” -WP243, del Grupo del Artículo 29, se indica expresamente que:

“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.”