agencia española protección datos

EL ESTATUTO DEL DELEGADO DE PROTECCIÓN DE DATOS

Orientaciones sobre el marco de actuación, independencia, garantías organizativas y conflictos de intereses



Guía publicada en
noviembre de 2026

Índice

PRESENTACIÓN 5
I. RESUMEN EJECUTIVO 9
II. DESIGNACIÓN DEL DPD 10
A. Cualidades profesionales del DPD 10
B. Proceso de designación del DPD 11
III. INDEPENDENCIA COMO GARANTÍA DE EFICACIA 19
A. Independencia funcional 20
B. Independencia jerárquica 20
C. Conflictos de interés 20
D. Independencia económica 21
E. Independencia organizativa 22
IV. REPORTE Y RENDICIÓN DE CUENTAS DEL DPD 23
El reporting del DPD como instrumento de gobernanza y responsabilidad proactiva 23
A. Mecanismos de reporte proporcionados al tamaño y complejidad de la organización 24
B. Comunicación directa con la alta dirección 25
C. Documentación del asesoramiento y trazabilidad de las decisiones 25
D. Comunicación de riesgos, incidencias y vulneraciones relevantes 26
E. Informes periódicos de actividad como buena práctica avanzada 26
Recursos organizativos necesarios para un reporting efectivo 27
V. GARANTÍAS CORPORATIVAS SOBRE EL NOMBRAMIENTO, LA PERMANENCIA Y EL CESE 27
A. La designación formal del DPD como garantía de independencia institucional 27
B. Participación del DPD en decisiones que afecten a su posición institucional... 28
C. La independencia del DPD como principio rector de su estatuto jurídico 29
D. Protección frente a la remoción y las medidas sancionadoras 30

E. Garantías reforzadas de permanencia 30

F. Motivación de las decisiones que afecten al DPD 31

G. Protección frente a medidas organizativas que afecten materialmente a la independencia del DPD 31

H. Protección frente a represalias y garantías organizativas mínimas 32

VI. EL DPD Y LA SUPERVISIÓN DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA .33

A. Políticas de protección de datos..... 34

B. Elaboración y mantenimiento actualizado del registro de actividades de tratamiento (RAT) y del inventario de actividades de tratamiento..... 35

C. Evaluación de impacto en protección de datos (EIPD)..... 37

D. Brechas de seguridad 38

E. Auditorías de protección de datos..... 39

VII. SITUACIONES QUE REQUIEREN UNA EVALUACIÓN ESPECÍFICA DE LA INDEPENDENCIA DEL DPD.....40

A. El DPD en los procesos de contratación 41

B. DPD con otros roles y responsabilidades en la organización 42

C. Posiciones en la organización potencialmente compatibles..... 45

D. Algunas situaciones que podrían comprometer la independencia del DPD o favorecer la existencia de posibles conflictos de intereses..... 47

VIII.VÍAS DE AMPARO DEL DPD 50

A. Consulta o denuncia ante la Autoridad de Control..... 51

B. Vía judicial..... 51

IX. CONCLUSIÓN 51

X. REFERENCIAS.....55

A. Agencia Española de Protección de Datos 55

B. Comité Europeo de Protección de Datos y Supervisor Europeo de Protección de Datos 56

C. Autoridades autonómicas..... 57

D. Autoridades de control de otros Estados 57

E. Asociaciones profesionales, estándares y otros 58

F. Jurisprudencia 59

PRESENTACIÓN

Las personas delegadas de protección de datos desempeñan una función esencial en el cumplimiento de la normativa de protección de datos personales y en la garantía de los derechos de las personas interesadas. No lo decimos como fórmula de cortesía. Lo afirmamos porque la protección de datos personales es hoy la garantía transversal de los derechos de las personas en el entorno digital, y porque esa garantía solo es efectiva si dentro de cada organización, pública o privada, hay alguien con el conocimiento, la posición y la independencia necesarios para asesorar con criterio y supervisar con objetividad. Para que su función sea efectiva es preciso que las organizaciones, tanto públicas como privadas, garanticen a quienes la ejercen la posición, los recursos —incluidos los necesarios para mantener sus conocimientos especializados— y la independencia que requieren un asesoramiento y una supervisión objetivos.

Esta función ocupa un lugar central en el Plan Estratégico 2025-2030 de la Agencia Española de Protección de Datos (AEPD). La elaboración del Plan se sustentó en medio centenar de reuniones con asociaciones profesionales, empresas, administraciones públicas, universidades y organizaciones de la sociedad civil, así como en una consulta pública que reunió cerca de medio millar de aportaciones, más de una quinta parte de ellas procedentes de profesionales de la privacidad. De ese proceso surgió el compromiso de consolidar la posición de las personas delegadas de protección de datos, reforzar su independencia funcional y su capacidad de actuación, y formular propuestas para clarificar su estatuto jurídico, incluidas las posibles incompatibilidades con otras funciones.

En este contexto se presenta «El estatuto del delegado de protección de datos. Orientaciones sobre el marco de actuación, independencia, garantías organizativas y conflictos de intereses», cuya elaboración exhaustiva y plural se ha prolongado durante cerca de un año. El borrador se sometió a dos rondas de consulta y diálogo con asociaciones profesionales y con personas que ejercen como delegadas de protección de datos en el sector público. Se recabaron, asimismo, las observaciones del Consejo de Transparencia y Protección de Datos de Andalucía, y el texto se puso a disposición de la Autoridad Catalana de Protección de Datos y de la Autoridad Vasca de Protección de Datos para su revisión.

Las aportaciones recibidas han permitido introducir modificaciones sustanciales, contrastar las orientaciones propuestas con la práctica profesional e identificar las dificultades y necesidades que plantea su aplicación. De este modo, han reforzado el fundamento técnico y la utilidad práctica del documento, que atiende a la diversidad de las organizaciones y a las condiciones reales del ejercicio profesional.

Este proceso se enmarca en el principio de «Agencia abierta» del Plan Estratégico 2025-2030 y contribuye al desarrollo de sus medidas 4.1, 4.2, 4.3 y 7.3, relativas, respectivamente, a la cooperación con los profesionales y sus organizaciones representativas; al refuerzo de la independencia y de la capacidad de actuación de las personas delegadas de protección de datos y a la clarificación de su estatuto jurídico; a la colaboración con las autoridades autonómicas y otros organismos competentes; y a la consulta y el diálogo previos a la publicación de guías y criterios, medida esta última integrada en el eje 7 del Plan, «Apertura, cercanía y cultura de protección de datos».

Este documento aborda la designación de la persona delegada de protección de datos; los criterios de independencia funcional, jerárquica, económica y organizativa; la rendición de cuentas ante la alta dirección; las garantías relativas al nombramiento, la permanencia y el cese; la supervisión del cumplimiento del principio de responsabilidad proactiva; la evaluación de posibles conflictos de intereses; y las vías de amparo disponibles.

Su finalidad es ofrecer criterios interpretativos que faciliten la aplicación de las garantías previstas en los artículos 37 a 39 del 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 en los artículos 34 a 37 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. En consecuencia, no introduce nuevas obligaciones ni impone un modelo organizativo único.

Sus orientaciones se dirigen tanto a las personas delegadas de protección de datos como a los responsables y encargados del tratamiento y a sus órganos de dirección. La independencia en el ejercicio de esta función constituye una garantía institucional cuya efectividad corresponde asegurar a cada organización.

En su elaboración se han tenido en cuenta el modelo de instrucción interna sobre el estatuto de la persona delegada de protección de datos del Consejo de Transparencia y Protección de Datos de Andalucía, que ha constituido un antecedente de especial relevancia; los documentos de referencia de las asociaciones profesionales; los informes y las resoluciones de la Agencia Española de Protección de Datos; y la jurisprudencia del Tribunal de Justicia de la Unión Europea y de la Audiencia Nacional.

Se han examinado, asimismo, los criterios y documentos del Comité Europeo de Protección de Datos y del Supervisor Europeo de Protección de Datos, así como los de las autoridades de control de Francia —Commission nationale de l'informatique et des libertés—, Bélgica —Autorité de protection des données / Gegevensbeschermingsautoriteit—, Italia —Garante per la protezione dei dati personali—, Países Bajos —Autoriteit Persoonsgegevens—, Irlanda —Data Protection Commission—, Finlandia —Tietosuojavaltuutetun toimisto—, Dinamarca —Datatilsynet— y Suecia —Integritetsskyddsmyndigheten—. Se han considerado también referencias internacionales, como la norma ISO 37009:2025, relativa a la gestión de los conflictos de intereses.

El texto podrá completarse a la luz de la experiencia derivada de su aplicación. En particular, está previsto elaborar, en colaboración con algunas de las asociaciones profesionales participantes, buenas prácticas para la prevención y resolución de conflictos de intereses en supuestos concretos. A tal fin, la Agencia mantendrá abiertos los cauces para recibir las observaciones y propuestas de mejora de quienes apliquen sus orientaciones.

Esta actuación se inscribe en un conjunto más amplio de iniciativas de cooperación con los profesionales de la privacidad. A lo largo de 2026, la Agencia ha mantenido un proceso de diálogo y colaboración con las personas delegadas de protección de datos de la Administración General del Estado, articulado en diversas reuniones con profesionales del sector público y privado, así como en un encuentro que congregó a más de setenta profesionales. De este proceso han derivado recomendaciones para reforzar el cumplimiento de la normativa de protección de datos en dicho ámbito, así como compromisos y actuaciones que se encuentran actualmente en ejecución.

Entre las próximas líneas de trabajo figura el análisis de la relación entre las funciones de protección de datos y las responsabilidades vinculadas a la inteligencia artificial. La aparición de nuevas funciones organizativas exige delimitar los respectivos ámbitos de actuación, prevenir posibles conflictos de intereses y preservar la independencia de las personas delegadas de protección de datos.

La Agencia Española de Protección de Datos agradece el tiempo y la experiencia aportados por las personas integrantes del Club del Delegado de Protección de Datos de la Asociación Española para la Calidad (AEC), la Asociación Profesional Española de Privacidad e Inteligencia Artificial (APEP·IA), la Asociación de Expertos Nacionales de la Abogacía TIC (ENATIC) y la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum), así como por las personas delegadas de protección de datos del sector público que han participado en este proceso. Extiende este reconocimiento a su personal y a los equipos que han intervenido en la preparación y revisión del documento.

Lorenzo Cotino Hueso

Presidente de la Agencia Española de Protección de Datos

Francisco Pérez Bes

Adjunto de la Agencia Española de Protección de Datos

I. RESUMEN EJECUTIVO

El Delegado de Protección de Datos (DPD) es la figura principal del modelo de cumplimiento del Reglamento General de Protección de Datos (RGPD) y de la Ley Orgánica 3/2018 de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), que son normas basadas –entre otros- en el principio de responsabilidad proactiva, que exige a los responsables y encargados no solo cumplir, sino también poder demostrarlo. Las funciones principales del DPD se recogen en el artículo 39 del RGPD, a las que se añaden las que le asigna el artículo 37 de la LOPDGDD, sin perjuicio de otras funciones y competencias que pueda asignarle el responsable o el encargado del tratamiento, siempre que no comprometan su independencia ni den lugar a conflicto de intereses.

La accesibilidad del DPD es, asimismo, una cualidad esencial para el correcto desempeño de sus competencias, por cuanto esta figura, en el ejercicio de sus funciones, actúa como nexo entre el responsable o encargado del tratamiento, la autoridad de control y los interesados.

Para cumplir eficazmente con su labor, el DPD debe operar con independencia, lo que significa que el responsable o el encargado del tratamiento deben garantizar que el DPD designado por ellos no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones: no se le puede indicar cómo abordar un asunto relacionado con la protección de datos, qué resultados debe lograr en sus análisis, cómo investigar una queja o reclamación, qué opinión debe mantener sobre la necesidad de consultar a la autoridad de control ni cómo debe interpretar la normativa. Ello implica que la independencia se exige en un sentido amplio, tanto respecto de la propia organización como respecto de otras organizaciones.

El Plan Estratégico 2025-2030 de la Agencia Española de Protección de Datos (AEPD) refuerza y enriquece la figura del DPD en varios aspectos clave, alineados con los retos tecnológicos, la transformación digital y la necesidad de garantizar un cumplimiento normativo robusto y proactivo. Con este fin, se pretende fortalecer la posición y la independencia del DPD, su integración en los flujos de toma de decisiones de las organizaciones y su formación y capacitación permanente, con enfoque tanto en la práctica del derecho como en las tecnologías emergentes. Pero, también, dotarle de herramientas adecuadas y suficientes y otros recursos de ayuda para, en definitiva, convertir al DPD en el eje principal de la cultura de protección de datos en las organizaciones, tanto públicas como privadas.

Afianzar la posición de los DPD mediante una serie de elementos que claramente refuercen su independencia, sus conocimientos y otras cualidades necesarias para su eficaz desempeño constituye uno de los principales retos a alcanzar. Así lo puso de manifiesto el Comité Europeo de Protección de Datos (CEPD) en el informe de la acción

de ejecución coordinada sobre la designación y posición de los DPD, de enero de 2024, en el que destacó, entre otros puntos de atención y recomendaciones, el conflicto de intereses y la falta de independencia del DPD. El informe también señalaba que las autoridades de control pueden adoptar orientaciones que incluyan también las nuevas funciones que asumen los DPD en virtud de los nuevos actos legislativos de la Unión Europea en el ámbito digital.

La presentación de estas orientaciones constituye una actuación destinada a integrar esta figura en las organizaciones y a facilitar la labor de los DPD en el marco de las disposiciones del RGPD y de la LOPDGDD que regulan su actividad, o de normativas sectoriales que impliquen tratamientos de datos en ámbitos específicos. Las previsiones aquí contempladas están dedicadas, principalmente, a la garantía de la independencia del DPD en el desempeño de sus funciones.

En consecuencia, el objetivo final de estas recomendaciones es dotar al DPD y a los responsables de las organizaciones que disponen de este tipo de servicios de un marco de certeza y seguridad jurídica que redunde en beneficio de la protección de los derechos y libertades de las personas físicas.

II. DESIGNACIÓN DEL DPD

El proceso de designación del DPD es un aspecto crítico para garantizar el cumplimiento del Reglamento General de Protección de Datos (RGPD) y de la Ley Orgánica 3/2018 de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD). A continuación, se detallan algunas de las consideraciones que, en general, es preciso tener en cuenta con carácter previo a su designación y, en particular, quién puede ser designado, cómo debe realizarse el proceso, cuáles son los requisitos legales y las funciones del DPD, así como las buenas prácticas recomendadas por el CEPD.

A. CUALIDADES PROFESIONALES DEL DPD

El artículo 37.5 del RGPD establece que el DPD debe ser designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos, así como a su capacidad para desempeñar las funciones que le asigna el RGPD. No obstante, en el contexto tecnológico actual, también es preciso recordar que el considerando 97[1] exige que el nivel de conocimientos especializados necesario se determine también en función del tipo de operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. En la práctica, deben tenerse igualmente en cuenta las cualidades profesionales relacionadas con su

[1] El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado.

experiencia en ingeniería de la privacidad, en privacidad y protección de datos, y sus conocimientos tecnológicos.

En particular, en relación con las operaciones de tratamiento llevadas a cabo por el responsable o el encargado, serán tenidas en consideración las posibles variables relativas al contexto, la naturaleza, los fines y el ámbito o alcance de estas. En la práctica, ello implica conocimientos jurídicos (RGPD, LOPDGDD, normas sectoriales, etc.), conocimientos técnicos (tecnologías emergentes, protección de datos desde el diseño y por defecto, medidas de seguridad, gestión de riesgos, etc.) y conocimientos organizativos (capacidad y habilidad para gestionar procesos internos, conocimiento de la organización, buenas prácticas en gobernanza, etc.), cuestiones que también se ponen de manifiesto en las directrices del CEPD[2].

La integración de esta figura en las organizaciones puede articularse mediante diferentes fórmulas: un empleado interno de la organización (ej.: abogado, responsable de cumplimiento, experto en TI); un profesional externo (ej.: consultor, abogado especializado, empresa de servicios de protección de datos); un equipo de personas (en organizaciones grandes, puede haber un equipo de protección de datos liderado por el DPD), o un DPD subcontratado a tiempo completo o a tiempo parcial (en este caso, la empresa contratada designa a una persona física como DPD para la organización cliente).

Además de los conocimientos especializados del Derecho y la práctica en materia de protección de datos, del conocimiento de la organización y sus procesos y del conocimiento de las características tecnológicas de las operaciones de tratamiento, hay que tener en consideración las denominadas habilidades blandas (*soft skills*), es decir, las competencias interpersonales necesarias para relacionarse con toda la organización ejerciendo el pensamiento crítico que requiere el trabajo de un DPD. Algunas de estas cualidades pueden ser la capacidad de comunicación y de trabajo en equipo, la capacidad para adaptarse a cambios e imprevistos, la empatía, la inteligencia emocional, la gestión del tiempo o las habilidades personales para la resolución de conflictos.

B. PROCESO DE DESIGNACIÓN DEL DPD

La designación del DPD puede realizarse mediante la creación de un órgano colegiado o mediante la designación de una persona determinada. La figura del órgano colegiado permite adecuarla a las características de la organización ya sea un organismo público o

[2] WP243: 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.

una entidad privada, por ejemplo, una UTE puede designar una oficina de protección de datos para ejercer las funciones del DPD para toda la UTE contando con personas de cada una de las entidades que la integran y, al mismo tiempo, dicha oficina puede contar con un asesoramiento externo contratado. Las ventajas del órgano colegiado son evidentes, no condiciona las funciones del DPD a la presencia física de una única persona y, en caso de conflicto de intereses, pueden implementarse mecanismos de abstención que no dificultarían el normal desarrollo de las funciones del DPD ni entorpecerían las actividades de las entidades responsables o encargadas.

Con independencia de que la designación recaiga en un órgano colegiado o en una persona física, el proceso de designación del DPD debe ser formal, documentado y transparente, y puede articularse en las siguientes fases:

1. Identificar la necesidad o la obligación de designar un DPD

Antes de designar un DPD, la organización debe evaluar si está obligada a hacerlo conforme al artículo 37 del RGPD y al artículo 34 de la LOPDGDD. Las situaciones que exigen la designación obligatoria de un DPD son:

- Organismos públicos (salvo tribunales en ejercicio de su función judicial).
- Tratamientos a gran escala de:
  - Datos personales sensibles (salud, ideología, afiliación sindical, etc.).
  - Datos relativos a condenas e infracciones penales.
- Observación habitual y sistemática de personas a gran escala (ej.: videovigilancia, perfiles de usuarios en redes sociales).
- Las entidades señaladas específicamente en el artículo 34[3] de la LOPDGDD.

[3] **Artículo 34. Designación de un delegado de protección de datos.**
1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:
a) Los colegios profesionales y sus consejos generales.
b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
f) Los establecimientos financieros de crédito.
g) Las entidades aseguradoras y reaseguradoras.
h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

2. Definir el perfil del DPD

La organización debe definir qué tipo de DPD necesita en función de:

- Tamaño de la organización: En una PYME, puede ser suficiente un DPD externo a tiempo parcial. En una gran empresa, debido a la complejidad y volumen de tratamientos, puede requerirse un equipo interno de protección de datos.
- Complejidad de los tratamientos: Si la organización trata datos sensibles o a gran escala, el DPD debe tener conocimientos técnicos avanzados.
- Sector de actividad: En sectores regulados (ej.: salud, banca, educación, etc.), es muy recomendable que el DPD tenga conocimientos específicos del sector.
- Conocimiento de la organización.

3. Parámetros para la evaluación de la posición de un DPD

Identificada la necesidad o la obligación de disponer de un DPD, y teniendo en cuenta el contexto, la naturaleza y el ámbito de la organización, algunos de los parámetros que pueden valorarse son los siguientes:

- Conocimientos y experiencia:
  - ¿Tiene formación acreditada y adecuada en protección de datos?
  - ¿Ha trabajado antes como DPD o en áreas relacionadas?

---

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
ñ) Las empresas de seguridad privada.
o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

- ¿Conoce el sector de actividad de la organización?

- Independencia:
  - ¿Puede actuar sin conflictos de intereses?
  - ¿Tiene acceso directo a la alta dirección?
  - ¿Existe algún equipo, unidad o personal dentro de la entidad, encargado de gestionar las cuestiones relativas a protección de datos que no correspondan a las funciones propias del DPD?
- Disponibilidad:
  - ¿Puede dedicar el tiempo necesario a las funciones de DPD?
  - En el caso de un DPD externo, ¿el contrato garantiza suficiente dedicación?
- Recursos:
  - ¿La organización puede proporcionar al DPD los recursos necesarios (herramientas, equipo, presupuesto)?[4]
- Certificaciones:
  - ¿Cuenta con certificación para DPD reconocida en el mercado o alguna certificación en privacidad o ingeniería de la privacidad?

4. Designación formal del DPD

Una vez seleccionado el candidato, la organización debe formalizar su designación. Este proceso puede realizarse mediante los siguientes pasos:

- Decisión de Designación
  - La designación del DPD debe ser aprobada por el órgano de gobierno de la organización.

Ejemplos:

- *en el sector público, por el consejo de gobierno, junta directiva u órgano equivalente;*
- *en el sector privado, por el consejo de administración, consejero delegado, director general o persona debidamente apoderada para ello con un poder especial.*

- Documentación de la Designación

[4] Este aspecto es especialmente relevante cuando el DPD se subcontrata a una organización externa.

La designación debe documentarse por escrito e incluir:

- **a)** Nombre y datos de contacto del DPD (teléfono, correo electrónico).
- **b)** Funciones del DPD (según el Art. 39 del RGPD).
- **c)** Ámbito de actuación y competencias (ej.: toda la organización, una división específica) así como otras funciones que le hubieran sido asignadas.
- **d)** Duración del nombramiento (si es temporal).
- **e)** Recursos asignados (presupuesto, equipo, herramientas).
- **f)** Garantías de independencia (ej.: acceso directo a la alta dirección, protección contra represalias y otras garantías, como las necesarias para evitar o gestionar los conflictos de intereses).

- Comunicación de la Designación

La organización debe comunicar la designación del DPD a:

- **a)** La Agencia Española de Protección de Datos (AEPD) mediante el proceso de registro habilitado para ello. En el caso de las comunidades autónomas con competencias en protección de datos, los organismos públicos deben comunicar la designación del DPD a sus respectivas autoridades de protección de datos.
- **b)** Los empleados de la organización:
  - El DPD debe ser conocido por todo el personal, especialmente por aquellos que tratan datos personales.
  - Se recomienda incluir su nombre y datos de contacto en la política de protección de datos de la organización, en las políticas de privacidad y en lugares comunes como la intranet, por ejemplo.
- **c)** Los interesados (clientes, usuarios, etc.):
  - El DPD debe figurar como punto de contacto en la información sobre protección de datos que se proporcione a los interesados (ej.: en la web, en contratos, en cláusulas de privacidad).
- **d)** Publicidad de los datos del DPD

Sin perjuicio de lo señalado en el punto anterior, debe tenerse en cuenta que el artículo 37.7 del RGPD establece que *"El responsable y el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control."* Es recomendable que la designación vaya acompañada de mecanismos internos de comunicación que permitan a todas las áreas de la organización conocer la existencia del DPD,

sus funciones y los canales habilitados para interactuar con él. Entre los medios que pueden tenerse en cuenta figuran:

- la web de la organización, el inventario de actividades de tratamiento, la política de privacidad, los procedimientos que la desarrollan o, preferiblemente, una sección dedicada a la protección de datos;
- los registros internos, como los registros de actividades de tratamiento (RAT);
- la documentación legal, los contratos, las cláusulas de privacidad y los avisos legales, etc.

e) Disponibilidad del DPD

La designación formal del DPD constituye una garantía esencial de transparencia y seguridad jurídica. Es recomendable que la política de protección de datos o la propia designación contemple de forma expresa aspectos relacionados con la continuidad de la función, particularmente en supuestos de ausencia temporal, sustitución o cese sobrevenido.

5. Funciones del DPD tras su designación

En la práctica, podría ocurrir que determinadas organizaciones interpreten que la designación formal de un DPD supone que todas las cuestiones relacionadas con la privacidad y la protección de datos pasan a ser responsabilidad exclusiva de esta figura. Esta interpretación resulta contraria al modelo de responsabilidad proactiva establecido por el RGPD y puede dar lugar a la atribución al DPD de funciones operativas, ejecutivas o decisorias incompatibles con su rol de asesoramiento y supervisión. En ningún caso, la designación formal de un DPD puede entenderse como una transferencia de la responsabilidad del cumplimiento normativo que el RGPD y la LOPDGDD asignan al responsable o al encargado del tratamiento.

Una vez designado, el DPD debe ejercer las funciones establecidas en el artículo 39 del RGPD, consistentes en:

- Informar y asesorar al responsable o encargado del tratamiento sobre sus obligaciones.
- Supervisar el cumplimiento del RGPD, la LOPDGDD y otras normativas sectoriales aplicables.
- Ofrecer asesoramiento sobre la evaluación de impacto (EIPD) y supervisar su aplicación.
- Cooperar con la AEPD y actuar como punto de contacto con la autoridad de control.

- Ser el punto de contacto para los interesados en relación con el tratamiento de sus datos.

6. Cese del DPD

Las designaciones a las que refiere el artículo 34 de la LOPDGDD[5] incluyen implícitamente los casos del cese del DPD y, por tanto, la obligación de responsables y encargados de comunicar a la autoridad de control tanto la designación como el cese, así como cualquier eventualidad que pueda implicar una modificación o actualización en relación con la comunicación previa efectuada. No prever de manera efectiva este procedimiento puede generar problemas prácticos, como mantener información incorrecta o desactualizada sobre el DPD o mantener al antiguo DPD como interlocutor visible ante la autoridad de control, los interesados o terceros pese a haber finalizado de manera efectiva su relación con la organización. Para prevenir eventuales ausencias del DPD o períodos transitorios de ausencia del mismo, una solución eficaz en la práctica es la de utilizar la fórmula del órgano colegiado (p ej. una “oficina de privacidad”), que permite garantizar la continuidad del servicio ante eventualidades sobrevenidas de ausencia del DPD.

Por su parte, el apartado 2 del artículo 36 de la LOPDGDD[6] establece que el DPD no puede ser removido ni sancionado por el responsable o el encargado por el mero desempeño de sus funciones, salvo que concurra dolo o negligencia grave. Esta previsión es especialmente destacable, ya que pone de relieve la necesidad de garantizar la independencia de sus funciones.

En este sentido, hay que tener en cuenta que si bien el responsable y el encargado deben garantizar la independencia del DPD en el ámbito del desempeño de sus funciones, ello no dota a la figura del DPD de un régimen de especial protección como el que el legislador atribuye a los representantes de los trabajadores o al responsable del servicio de prevención de riesgos laborales[7], pues "*No es la independencia en el ejercicio de una función sino la función en si misma lo que hace que la RLT tengan una mayor protección frente al despido y que se equipare a la misma a los delegados de prevención de riesgos de acuerdo con el artículo 30. 4 de la LPRL.*[8]".

[5] Art. 34 LOPDGDD apartado 3: Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

[6] Art. 36 LOPDGDD apartado 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

[7] Sentencia STSJ M 7356/2026 - ECLI:ES:TSJM:2026:7356

[8] Art. 30 LPRL apartado 4: Los trabajadores designados no podrán sufrir ningún perjuicio derivado de sus actividades de protección y prevención de los riesgos profesionales en la empresa. En ejercicio de esta función, dichos trabajadores gozarán, en particular, de las garantías que para los representantes de los trabajadores establecen las

7. Buenas prácticas en la designación del DPD

El CEPD y la AEPD consideran buenas prácticas para garantizar una designación efectiva del DPD, al menos, las siguientes:

- Designar al DPD en un nivel administrativo elevado (ej.: nivel 28-30 en la Administración General del Estado, como garantía de la interlocución al más alto nivel).
- Como buena práctica organizativa, se recomienda formalizar el nombramiento del DPD mediante una Carta de Misión, cuando se trate de un DPD interno, o mediante la correspondiente regulación contractual (en el ámbito privado o en los pliegos en la contratación pública) cuando el servicio sea prestado por un DPD externo.
- Este documento podrá recoger, entre otras cuestiones, las funciones asignadas al DPD, los mecanismos de reporte directo a los órganos de dirección, los procedimientos de consulta temprana en materia de protección de datos, los recursos puestos a su disposición, las garantías de independencia y el plan de actuación o supervisión previsto para el ejercicio de sus funciones.
- Incluir al DPD en el organigrama de la organización para garantizar su visibilidad.
- Crear una oficina o comité de protección de datos para asegurar la continuidad del rol del DPD, de modo que no se vea afectada por la rotación o ausencia de personal.
- Evaluar conflictos de intereses antes de la designación.
- Designar al DPD por el consejo de administración o la dirección general.
- Garantizar que el DPD reporte directamente a la alta dirección.
- Evitar que el DPD tenga funciones operativas que puedan generar conflictos de intereses.
- Proporcionarle recursos suficientes (presupuesto, herramientas, equipo).
- Para DPD externos: firmar un contrato claro que defina las funciones del DPD, las garantías de independencia, la duración del servicio y los recursos asignados.

En definitiva, la designación deberá asegurar que el DPD tenga acceso a toda la información necesaria para ejercer sus funciones con independencia, y debe atender no solo a su cualificación profesional, sino también a las condiciones reales de ejercicio de sus funciones y a las garantías de independencia. En este sentido, la Sentencia de la Audiencia Nacional 139/2026, de 18 de marzo de 2026 (ECLI:ES:AN:2026:1355), confirma

letras a), b) y c) del artículo 68 y el apartado 4 del artículo 56 del texto refundido de la Ley del Estatuto de los Trabajadores.

la necesidad de examinar las funciones efectivamente atribuidas a la persona designada, especialmente cuando participa en decisiones que determinan los fines y medios de los tratamientos que posteriormente debe supervisar (art. 38.6 RGPD).

III. INDEPENDENCIA COMO GARANTÍA DE EFICACIA

La independencia del DPD es una de las garantías fundamentales que establece el RGPD en su artículo 38.3 y que desarrollan las directrices del CEPD y las recomendaciones[9] de la AEPD. Esta independencia garantiza que el DPD pueda ejercer sus funciones de supervisión, asesoramiento y control sin presiones externas, conflictos de intereses o influencias que puedan comprometer su objetividad.

A continuación, se detalla qué implica la independencia del DPD, cómo se puede garantizar y qué requisitos debe cumplir, según el marco normativo y las buenas prácticas recomendadas por la AEPD y el CEPD.

El artículo 38.3 del RGPD establece 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 será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones."* En definitiva, el DPD no puede recibir instrucciones sobre cómo ejercer sus funciones ni puede ser destituido o sancionado por cumplir con su labor de supervisión y asesoramiento.

Por otra parte, el apartado quinto del artículo 38 del RGPD determina que *"El delegado de protección de datos estará vinculado por el secreto o la confidencialidad en el desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros."*, lo que viene a reforzar la idea de que las actuaciones del DPD se deben realizar sin interferencias que le impidan el acceso a toda la información que le sea necesaria.

Por su parte, la LOPDGDD refuerza el marco del RGPD y establece que el DPD debe actuar con autonomía y sin conflictos de intereses (artículo 36), prohibiendo cualquier presión o influencia que pueda afectar a su independencia.

Las Directrices del CEPD destacan que la independencia del DPD es esencial para garantizar su credibilidad y eficacia, lo que hace necesario que pueda actuar sin temor a represalias y con acceso directo al más alto nivel de la organización (ej.: consejo de administración, dirección general, etc.). En la práctica, esta independencia se podría resumir en los siguientes requisitos:

[9] https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-impulsa-un-modelo-comun-de-cumplimiento-en-el-sector

A. INDEPENDENCIA FUNCIONAL

- **No recibir instrucciones sobre sus funciones**: el DPD no puede ser obligado a adoptar una postura concreta en materia de protección de datos. Por ejemplo**,** si el DPD identifica y evalúa un riesgo en un tratamiento de datos, no puede ser presionado para minimizarlo, ignorarlo**,** evitarlo o reconsiderar su evaluación.
- El DPD debe poder emitir informes, recomendaciones y alertas sin que estos sean modificados o censurados por la organización. Por ejemplo, si el DPD emite un informe sobre el incumplimiento de una evaluación de impacto (EIPD), este debe ser respetado y considerado por la dirección.

B. INDEPENDENCIA JERÁRQUICA

- **Posición en el organigrama**: el DPD debe reportar directamente al más alto nivel de la organización (ej.: consejo de administración, director general, comité de dirección).
- *En el sector público: debe depender de un órgano con capacidad decisoria (ej.: Subsecretaría, Secretaría General).*

En el sector privado: debe informar directamente a la dirección general o al consejo de administración. En organizaciones con órganos de administración y órganos de dirección diferenciados, se recomienda que el DPD reporte a ambos niveles jerárquicos.

C. CONFLICTOS DE INTERÉS

- La Organización Internacional de Normalización[10] publicó en septiembre de 2025 su norma ISO 37009, con el título "Conflict of interest in organizations" (ISO 37009:2025). Esta norma ofrece orientaciones generales para entender el conflicto de intereses, identificarlo y gestionarlo en cualquier tipo de organización, tanto si se trata de un conflicto de intereses potencial, percibido o real que pueda obstaculizar los objetivos de una organización o las funciones de cualquiera de sus integrantes, como podría ser el caso del DPD.
- La adecuada gestión del conflicto de intereses, alineada con la ISO 37009:2025, es clave para la confianza y reputación de la organización. Su alcance es general y no se circunscribe únicamente al ámbito de la lucha contra la corrupción, siendo un elemento esencial para garantizar que cualquier proceso de toma de decisiones sea íntegro y eficaz. Partiendo de lo anterior, y con el objetivo de evitar el conflicto de intereses, es preciso que los responsables elaboren normas

[10] ISO: International Organization for Standardization, **organismo** independiente, no gubernamental, que reúne a expertos de más de 160 países con el objetivo de desarrollar normas internacionales **destinadas** a garantizar la calidad, seguridad, eficiencia y compatibilidad de productos**,** servicios y sistemas.

internas que posibiliten la identificación y la adecuada gestión de eventuales conflictos de intereses.

- El RGPD admite que el DPD sea interno o externo a la organización obligada a designarlo. En ambos casos**,** el responsable o encargado del tratamiento garantizará que las funciones y cometidos del DPD no se vean afectados por un potencial conflicto de intereses.
- El DPD no puede desempeñar funciones que puedan entrar en conflicto con su rol de supervisión. El conflicto de intereses puede aparecer en la designación del DPD, en el desarrollo de sus funciones, en el ejercicio de otros roles o funciones asignados por el responsable o en cualquier otro momento.

Son ejemplos de conflictos de intereses, entre otros, los siguientes:

- Ser responsable de un departamento que trata datos personales (ej.: director de marketing, RR.HH. o TI).
- Asumir funciones que impliquen poder decisorio sobre la determinación o aprobación de los fines y medios de los tratamientos de datos o de sus operaciones (p. ej., adoptar la decisión final sobre la implantación y configuración de un sistema de videovigilancia).

Como parte fundamental del principio de responsabilidad proactiva, se recomienda que la organización cuente con normas previas al nombramiento del DPD con el objetivo de determinar qué conflictos de intereses concretos pueden generarse en la organización, qué hacer con situaciones no previstas de conflicto de intereses y cómo gestionarlo.

D. INDEPENDENCIA ECONÓMICA

La suficiencia de recursos constituye un elemento esencial para garantizar el adecuado desempeño de las funciones del DPD. No obstante, la valoración de estos recursos debe efectuarse teniendo en cuenta el tamaño, la complejidad y las características de cada organización.

La autonomía financiera es igualmente esencial para garantizar la independencia efectiva del DPD, ya que su ausencia puede limitar, por ejemplo, su acceso a la formación adecuada o a la asistencia especializada de recursos como herramientas de soporte o la asistencia de especialistas externos. En general:

- El DPD debe tener una remuneración adecuada y estabilidad en el puesto para evitar presiones económicas.
- No puede ser destituido por cumplir con sus funciones (art. 38.3 RGPD); su destitución deberá justificarse sobre la base de un posible incumplimiento grave de sus obligaciones y no por discrepar de la organización. En este sentido, la posible destitución del DPD puede interpretarse como una presión implícita en términos de remuneración y estabilidad.

- No debe tener intereses relevantes o de control en los tratamientos de datos de los que pueda depender en términos de beneficios. Por ejemplo**,** si el DPD es accionista mayoritario de una empresa que proporciona servicios de tratamiento de datos a su organización, esto podría afectar a su independencia. También podría afectar a su independencia un bonus o una retribución variable vinculada a resultados económicos o al beneficio empresarial**,** dado que podría influir en su objetividad.

E. INDEPENDENCIA ORGANIZATIVA

Las funciones del DPD no pueden obstaculizarse o impedirse por la estructura organizativa. Su posición orgánica debe garantizar:

- Su acceso material a todos los datos, procesos y sistemas necesarios para ejercer sus funciones. Por ejemplo, acceso a los registros de actividades de tratamiento (RAT), evaluaciones de impacto, contratos con encargados de tratamiento, etc.
- Que cuente con los medios necesarios proporcionados por la organización: recursos humanos (equipo de apoyo, si fuera necesario), recursos técnicos (herramientas de análisis, software de gestión, etc.) y presupuesto para formación y asistencia externa, si fuera precisa (asesoría legal y técnica).
- Su implicación y participación en decisiones estratégicas: el DPD debe ser consultado de forma temprana en proyectos que impliquen tratamientos de datos (art. 38.1 RGPD). Por ejemplo, debe participar con su asesoramiento en la fase de diseño de un nuevo sistema de IA que trate datos personales.

Las Recomendaciones AEPD para el sector público proponen:

- que el DPD sea incluido en la estructura de la organización con un nivel administrativo elevado (ej.: nivel 28-30);
- que su designación formal sea pública y esté documentada de forma transparente, con una descripción clara de sus funciones y límites;
- la creación de estructuras estables, como las oficinas o comités de protección de datos, para garantizar la continuidad del rol del DPD incluso cuando se produzcan cambios de personal; y
- el análisis de los conflictos de intereses antes de designar al DPD.

En cuanto al sector privado, el DPD puede ser nombrado por el consejo de administración o por el director general. Si es externo, puede designarse mediante un contrato específico que garantice su independencia, de manera que no reciba instrucciones en el ejercicio de sus funciones, mediante la inclusión de las correspondientes cláusulas contractuales.

Una buena práctica, tanto en el sector privado como en el público, puede consistir en que el DPD elabore un informe anual dirigido a la alta dirección sobre el cumplimiento de la protección de datos**,** sin que este pueda ser modificado o censurado.

Otra buena práctica consiste en incluir en las auditorías de protección de datos el análisis de la independencia del DPD.

El DPD debe tener acceso al canal del informante, a través del cual podrá reportar presiones o posibles conflictos de intereses que afecten o puedan afectar a su independencia en el ejercicio de sus funciones.

IV. REPORTE Y RENDICIÓN DE CUENTAS DEL DPD

La AEPD considera una buena práctica promover mecanismos de reporte del DPD adaptados a las características de cada organización, que aseguren su comunicación efectiva con el máximo nivel de dirección, pero no prescribe un modelo de reporte específico o general. Sea cual sea el modelo de reporte de la organización deberá garantizar la segregación de las funciones de asesoramiento y supervisión del DPD y su independencia frente a cualquier función que implique poder decisorio en los tratamientos de datos personales.

Esta orientación encuentra un respaldo especialmente directo en el Informe del CEPD sobre la acción coordinada relativa a la designación y posición de los DPD, de enero de 2024, cuyo apartado 4.6 identifica las dificultades de acceso a la alta dirección y contempla expresamente la elaboración de recomendaciones o modelos adaptables de reporting, incluso con periodicidad anual, como posibles buenas prácticas institucionales.

En la misma línea, la CNIL francesa, mediante su guía y modelo de informe de actividad publicados el 27 de abril de 2026, ha desarrollado una herramienta de seguimiento de la actividad y comunicación con la dirección, cuya utilización recomienda sin considerarla jurídicamente obligatoria. Ambos documentos respaldan la conveniencia de promover sistemas proporcionados y útiles de reporting, manteniendo la flexibilidad organizativa y evitando que la documentación se convierta en una finalidad autónoma.

EL REPORTING DEL DPD COMO INSTRUMENTO DE GOBERNANZA Y RESPONSABILIDAD PROACTIVA

El reporte o rendición de cuentas del DPD debe articularse en función de la estructura, tamaño y complejidad de la organización, su sector de actividad y la normativa que le sea aplicable y constituye una manifestación directa del principio de responsabilidad proactiva y una condición necesaria para la efectividad de las funciones mínimas que el RGPD atribuye al DPD. Aunque el Reglamento General de Protección de Datos no impone la elaboración de una memoria anual ni establece un modelo formal de informe periódico, sí exige que el DPD participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos, disponga de acceso a la

información necesaria para el desempeño de sus funciones y reporte directamente al más alto nivel jerárquico de la organización[11].

Estas exigencias deben traducirse en mecanismos efectivos de interlocución entre el DPD y los órganos de dirección que permitan trasladar riesgos, recomendaciones, necesidades de cumplimiento y cuestiones relevantes para la protección de datos[12]. La finalidad de estos mecanismos no debe ser incrementar la carga documental de las organizaciones ni del propio DPD, sino asegurar que la dirección dispone de la información necesaria para adoptar decisiones informadas y que puede acreditarse la participación efectiva del DPD en la gobernanza de la protección de datos.

A. MECANISMOS DE REPORTE PROPORCIONADOS AL TAMAÑO Y COMPLEJIDAD DE LA ORGANIZACIÓN

No existe un único modelo válido de reporte del DPD, conclusión que resulta coherente con la ausencia de una regulación específica en el RGPD sobre formatos de reporte y con la diversidad de soluciones observadas en las orientaciones de la CNIL, la autoridad finlandesa, la autoridad irlandesa y el SEPD.

Los mecanismos de comunicación y rendición de cuentas deben adaptarse a la naturaleza, dimensión, complejidad y nivel de riesgo de los tratamientos realizados por cada organización para dar cumplimiento al principio general de responsabilidad proactiva y, en particular, al enfoque basado en riesgo del RGPD.

En organizaciones de gran tamaño, con estructuras complejas, tratamientos intensivos de datos personales o actividades que comporten riesgos significativos para los derechos y libertades de las personas, puede resultar aconsejable establecer mecanismos periódicos de reporte formalizados e incluso informes estructurados dirigidos a la alta dirección[13]. Por el contrario, en organizaciones de menor dimensión o con tratamientos menos complejos, la trazabilidad de la actividad del DPD puede alcanzarse mediante mecanismos más sencillos, como actas de reuniones, comunicaciones documentadas, registros de recomendaciones o informes específicos sobre cuestiones relevantes[14].

El criterio determinante no debería ser la existencia de un formato documental concreto, sino la capacidad de acreditar que el DPD ha podido ejercer sus funciones, comunicar sus recomendaciones y trasladar a la dirección los riesgos o incidencias relevantes identificados en el ejercicio de sus funciones.

[11] Arts. 38 y 39 RGPD; Directrices WP243/CEPD; Guía del SEPD sobre el papel del DPO en instituciones y organismos de la Unión Europea.
[12] Directrices WP243/CEPD; Coordinated Enforcement Action del CEPD sobre designación y posición del DPO; Guía SEPD 2025.
[13] **Por ejemplo,** el modelo CNIL: https://www.cnil.fr/fr/rapport-activite-dpo
[14] Orientaciones de Finlandia e Irlanda y modelos profesionales del BvD.

B. COMUNICACIÓN DIRECTA CON LA ALTA DIRECCIÓN

La obligación prevista en el artículo 38.3 RGPD de que el DPD reporte directamente al más alto nivel jerárquico debe interpretarse como una garantía material de independencia y no como una mera previsión formal de organigrama. Las organizaciones deben establecer cauces estables para que el DPD pueda comunicar directamente a la dirección cuestiones relevantes relacionadas con el cumplimiento de la normativa de protección de datos, sin filtros indebidos, obstáculos ni intermediarios[15].

Resulta especialmente recomendable definir internamente los procedimientos de elevación de riesgos, la forma de comunicar incidencias significativas y los mecanismos de seguimiento de las recomendaciones formuladas por el DPD. Con carácter general, la efectividad de la función del DPD depende, en gran medida, de la existencia de una interlocución real con los órganos de dirección y de la capacidad de trasladar alertas o recomendaciones antes de que los riesgos lleguen a materializarse.

En general, se recomienda que el marco de desempeño del DPD se integre en el proceso de su designación y se defina desde la política de protección de datos del responsable, identificando funciones, ámbito de actuación, recursos, garantías de independencia y vías de reporte**,** sin perjuicio de los posibles informes periódicos, de las comunicaciones extraordinarias que pudieran resultar necesarias ante brechas de datos relevantes o riesgos elevados, o de las actuaciones que pudiera realizar ante la autoridad de control.

C. DOCUMENTACIÓN DEL ASESORAMIENTO Y TRAZABILIDAD DE LAS DECISIONES

Una de las garantías más eficaces para reforzar la independencia y utilidad del DPD consiste en documentar adecuadamente las actuaciones de asesoramiento y supervisión que desarrolla. No se trata de generar cargas documentales innecesarias, sino de asegurar una trazabilidad razonable de las cuestiones relevantes que permitan acreditar la intervención del DPD y el cumplimiento de las obligaciones de responsabilidad proactiva. Por ello, resulta recomendable conservar evidencia suficiente de:

- las consultas relevantes planteadas al DPD;
- el asesoramiento emitido;
- las recomendaciones formuladas;
- las decisiones finalmente adoptadas por la organización cuando afecten a cuestiones relevantes de protección de datos; y
- las actuaciones de supervisión realizadas.

[15] Directrices WP243/CEPD; Guidance EDPS 2025; Coordinated Enforcement Action del CEPD

La experiencia comparada europea muestra además una tendencia creciente a documentar las situaciones en las que la organización decide apartarse del criterio expresado por el DPD. Esta práctica constituye una garantía especialmente útil para reforzar la trazabilidad de la toma de decisiones y facilitar la rendición de cuentas, sin alterar el carácter no vinculante de las recomendaciones del DPD.

D. COMUNICACIÓN DE RIESGOS, INCIDENCIAS Y VULNERACIONES RELEVANTES

La actividad de reporte del DPD no debe limitarse a mecanismos periódicos de información**,** pues determinadas circunstancias exigen una comunicación inmediata a los órganos de administración y dirección. En este sentido, el artículo 36.4 LOPDGDD establece expresamente la obligación de documentar y comunicar las vulneraciones relevantes en materia de protección de datos, previsión que refleja una idea más amplia: la dirección debe conocer oportunamente aquellas situaciones que puedan comprometer de forma significativa el cumplimiento normativo, la protección de los derechos de las personas afectadas o la propia posición de la organización[16].

Por ello, resulta recomendable que los mecanismos internos permitan al DPD elevar de forma inmediata riesgos significativos, incumplimientos relevantes, deficiencias estructurales o necesidades organizativas que requieran una actuación de la dirección.

E. INFORMES PERIÓDICOS DE ACTIVIDAD COMO BUENA PRÁCTICA AVANZADA

La elaboración de informes periódicos de actividad constituye una buena práctica de gobernanza particularmente útil en organizaciones complejas, pero no una obligación jurídica general derivada del RGPD.

La iniciativa[17] desarrollada por la CNIL francesa mediante la publicación de una guía específica y un modelo de informe de actividad del DPO constituye una referencia especialmente valiosa para aquellas organizaciones que deseen reforzar sus mecanismos de gobernanza y rendición de cuentas.

Estos informes pueden contribuir a ofrecer una visión estructurada del estado de cumplimiento de la organización, facilitar la planificación de actuaciones futuras y asegurar la continuidad de la función del DPD.

Se recomienda que los posibles modelos de informes se orienten a facilitar la toma de decisiones por la dirección y no a generar documentación meramente formal. Su contenido debería ser proporcionado a las características de la organización y centrarse en los principales riesgos, actuaciones realizadas, recomendaciones formuladas y necesidades detectadas.

[16] Esta previsión del apartado 4 del Art. 36 de la **LOPDGDD** se encuentra plenamente reforzada por las Directrices WP243/CEPD; Guidance EDPS 2025 y CNIL.
[17] (arts. 38 y 39 RGPD; modelo CNIL sobre rapport d'activité du DPO).

RECURSOS ORGANIZATIVOS NECESARIOS PARA UN REPORTING EFECTIVO

La rendición de cuentas del DPD solo puede resultar efectiva cuando la organización garantiza las condiciones necesarias para el ejercicio de sus funciones. En todo caso, los mecanismos de reporte, o los recursos y medios puestos a disposición del DPD, deben evaluarse atendiendo a las características específicas de cada organización, incluyendo su tamaño, naturaleza, estructura organizativa, volumen de tratamientos y nivel de complejidad.

Estas garantías no persiguen incrementar las obligaciones documentales de las organizaciones, sino asegurar que el DPD puede desarrollar una supervisión efectiva y trasladar oportunamente, en tiempo y forma, a la dirección las cuestiones que requieran su atención.

El objetivo del sistema europeo no es imponer modelos uniformes de reporte o memorias periódicas obligatorias, sino garantizar que exista una comunicación efectiva, documentada y proporcionada entre el DPD y la alta dirección. La forma concreta que adopte dicha comunicación puede variar en función de las características de cada organización. Lo relevante es que permita acreditar la participación efectiva del DPD, la adecuada consideración de sus recomendaciones y la integración de la protección de datos en los procesos de decisión y gobernanza de la entidad.

V. GARANTÍAS CORPORATIVAS SOBRE EL NOMBRAMIENTO, LA PERMANENCIA Y EL CESE

A. LA DESIGNACIÓN FORMAL DEL DPD COMO GARANTÍA DE INDEPENDENCIA INSTITUCIONAL

La designación del DPD no constituye un mero trámite organizativo, sino una garantía institucional esencial para la efectividad del sistema de protección de datos. La obligación de designar un DPD cuando concurran los supuestos previstos en el artículo 37 RGPD debe interpretarse conjuntamente con los artículos 38 y 39 RGPD. La finalidad de la designación no es únicamente identificar a una persona responsable de determinadas funciones, sino garantizar que la organización disponga de un interlocutor especializado, independiente y adecuadamente integrado en sus procesos de gobernanza.

Por ello, el nombramiento del DPD debería formalizarse siempre mediante un acto expreso, escrito y suficientemente documentado, con independencia de que la organización se encuentre, o no, sujeta a procedimientos internos específicos de designación.

Resulta especialmente recomendable que dicho acto identifique de manera expresa:

- la persona física o entidad designada;

- la fecha de efectos del nombramiento;
- la posición organizativa del DPD;
- sus canales de reporte;
- los medios y recursos inicialmente asignados para el desempeño de sus funciones;
- la forma en que se garantizará su acceso a la alta dirección.

Esta orientación resulta coherente con el régimen previsto en los artículos 34 a 37 LOPDGDD, con las exigencias organizativas derivadas de los artículos 38 y 39 RGPD y con las orientaciones recogidas en las Directrices WP243 sobre Delegados de Protección de Datos del CEPD, en la Coordinated Enforcement Action del CEPD sobre designación y posición del DPO y en la Guidance on the role of Data Protection Officers del SEPD.

Asimismo, la experiencia comparada europea muestra una tendencia creciente a complementar el nombramiento formal mediante documentos que definan expresamente funciones, responsabilidades, posición organizativa y mecanismos de reporte, tendencia observable en el Documento di indirizzo del Garante italiano de 2021 y en los criterios neerlandeses sobre la posición institucional del FG. Aunque esta práctica no constituye actualmente una obligación jurídica general, la AEPD considera que representa una garantía especialmente adecuada para prevenir conflictos posteriores sobre el alcance de las funciones del DPD y sobre su posición dentro de la organización.

B. PARTICIPACIÓN DEL DPD EN DECISIONES QUE AFECTEN A SU POSICIÓN INSTITUCIONAL

La participación adecuada y en tiempo oportuno del DPD, mediante su asesoramiento y supervisión, en todas las cuestiones relativas a la protección de datos constituye una exigencia expresa del artículo 38.1 RGPD. Esta garantía debe proyectarse también sobre aquellas decisiones organizativas que afecten directamente a la posición, funciones, estructura de apoyo o capacidad de actuación del propio DPD.

En esta materia resulta particularmente relevante el criterio mantenido por la AEPD en su Informe Jurídico 0038/2023, según el cual, cuando una reorganización interna incida sobre las funciones o posición institucional del DPD, resulta procedente recabar su parecer con carácter previo. Aunque dicho parecer no tenga carácter vinculante, la organización debe seguir garantizando el cumplimiento efectivo de las exigencias derivadas del RGPD respecto de la posición y funciones del DPD.

Además, es recomendable que las organizaciones documenten tanto el análisis realizado como las razones que justifican la decisión finalmente adoptada cuando esta se aparte del criterio expresado por el DPD. Esta recomendación encuentra apoyo en el propio Informe Jurídico 0038/2023, en las orientaciones de la autoridad irlandesa sobre

gobernanza y trazabilidad del asesoramiento del DPO, en las recomendaciones formuladas por la autoridad finlandesa y en los desarrollos recientes de la CNIL sobre reporting y rendición de cuentas del DPO.

Esta práctica no atribuye carácter vinculante a las recomendaciones del DPD ni desplaza a este la responsabilidad correspondiente al responsable o encargado del tratamiento, sino que favorece la transparencia del proceso decisorio y la acreditación del cumplimiento.

En concreto, esta recomendación tiene un respaldo directo en las Directrices sobre Delegados de Protección de Datos del Grupo de Trabajo del Artículo 29 (WP243 rev.01), asumidas por el CEPD, y en el Informe Jurídico 0038/2023 de la AEPD, que examina tanto la necesidad de documentar los motivos por los que no se sigue el consejo del DPD como su participación en las reorganizaciones que afectan a su posición y funciones (pp. 26 y 29). Asimismo, la Data Protection Commission irlandesa, en su decisión de 10 de mayo de 2021 sobre el Department of Employment Affairs and Social Protection (IN-18-12-01, apartados 6.8 a 6.13, especialmente 6.10), considera que la participación adecuada del DPD exige tomar efectivamente en consideración su asesoramiento y recoge la recomendación de documentar las razones por las que este no se sigue. El modelo de informe de actividad publicado por la CNIL en 2026 constituye, por su parte, un instrumento complementario para sistematizar el seguimiento de recomendaciones y decisiones.

C. LA INDEPENDENCIA DEL DPD COMO PRINCIPIO RECTOR DE SU ESTATUTO JURÍDICO

El núcleo del estatuto jurídico del DPD no reside en la atribución de una inamovilidad absoluta, sino en la protección efectiva de su independencia funcional. Los artículos 38.1, 38.2 y 38.3 RGPD, interpretados conjuntamente con el considerando 97, deben entenderse como un conjunto de garantías destinadas a asegurar que el DPD pueda ejercer sus funciones de supervisión, asesoramiento y control sin recibir instrucciones sobre el contenido de su actuación ni sufrir consecuencias desfavorables derivadas del ejercicio de sus funciones.

Esta interpretación resulta coherente con las Directrices WP243 rev.01**,** posteriormente asumidas por el CEPD, con la Guía del SEPD sobre el papel del DPO en las instituciones europeas y con una práctica convergente observada en numerosas autoridades europeas, entre ellas la CNIL francesa, la Autoridad belga de Protección de Datos, la autoridad danesa y la autoridad sueca, todas ellas particularmente insistentes en la independencia funcional como presupuesto del correcto ejercicio de la función. En consecuencia, toda interpretación del estatuto jurídico del DPD debe realizarse a la luz de este principio general de independencia funcional.

D. PROTECCIÓN FRENTE A LA REMOCIÓN Y LAS MEDIDAS SANCIONADORAS

El artículo 38.3 RGPD establece que el DPD no podrá ser destituido ni sancionado por desempeñar sus funciones. Esta garantía ha sido interpretada por el Tribunal de Justicia de la Unión Europea en las sentencias Leistritz, de 22 de junio de 2022 (C-534/20, ECLI:EU:C:2022:495), X-FAB Dresden, de 9 de febrero de 2023 (C-453/21, ECLI:EU:C:2023:79), y KISA, de 9 de febrero de 2023 (C-560/21, ECLI:EU:C:2023:81).

En Leistritz, el Tribunal precisó que la prohibición del artículo 38.3 RGPD protege al DPD frente a decisiones que pongan fin a sus funciones, le sean desfavorables o constituyan una sanción, siempre que estén vinculadas al desempeño de las funciones que tiene encomendadas. Esta protección no supone una inamovilidad absoluta ni impide adoptar decisiones legítimas basadas en causas ajenas al ejercicio de dichas funciones.

Las sentencias Leistritz, X-FAB Dresden y KISA confirman -asimismo- que el Derecho nacional puede establecer garantías reforzadas frente a la remoción del DPD, incluida la exigencia de una causa grave, siempre que tales garantías no comprometan los objetivos del RGPD. Esta jurisprudencia respalda una interpretación efectiva de la independencia funcional del DPD y la conveniencia de que cualquier decisión de cese pueda justificarse por circunstancias objetivas, diferenciadas del ejercicio independiente de sus funciones.

A la luz de esta jurisprudencia, cualquier medida que afecte negativamente a la posición profesional del DPD debe poder justificarse mediante razones objetivas ajenas al ejercicio de sus funciones de supervisión, asesoramiento o control. La protección prevista por el artículo 38.3 RGPD debe interpretarse de manera funcional y no meramente formal.

E. GARANTÍAS REFORZADAS DE PERMANENCIA

El artículo 36.2 de la LOPDGDD constituye una de las manifestaciones más relevantes de la protección reforzada del DPD en el ámbito europeo: cuando el DPD sea una persona física integrada en la organización, la remoción o sanción solo puede justificarse por la existencia de dolo o negligencia grave en el ejercicio de sus funciones. Esta previsión debe interpretarse como una garantía institucional destinada a proteger la independencia del DPD frente a presiones organizativas derivadas del contenido de sus actuaciones o recomendaciones.

Las sentencias Leistritz (C-534/20) y X-FAB Dresden (C-453/21) han confirmado expresamente que los Estados miembros pueden establecer niveles de protección superiores a los previstos por el RGPD siempre que no comprometan los objetivos del Reglamento. Por tanto, esta posibilidad de protección reforzada constituye un elemento legítimo y compatible con el modelo europeo de gobernanza en protección de datos.

La experiencia comparada muestra que algunos ordenamientos han desarrollado mecanismos aún más intensos de estabilidad funcional. Destaca especialmente el modelo alemán, en el que la BDSG condiciona la revocación del DPD a la concurrencia de

una causa grave y remite, por analogía, al régimen del artículo 626 del Código Civil alemán (BGB), relativo a la resolución extraordinaria de relaciones jurídicas basadas en una especial relación de confianza. A ello se añade una protección adicional frente a determinadas decisiones posteriores que afecten a la continuidad de la relación laboral. Aunque estas soluciones responden a opciones normativas nacionales específicas, ponen de manifiesto que el fortalecimiento de las garantías de permanencia constituye una vía legítima para reforzar la independencia efectiva del DPD. No obstante, estas garantías no suponen una inamovilidad absoluta ni limitan la capacidad organizativa de la entidad cuando concurran causas legítimas ajenas al ejercicio de sus funciones.

F. MOTIVACIÓN DE LAS DECISIONES QUE AFECTEN AL DPD

Toda decisión que afecte de forma significativa a la posición institucional del DPD debería estar suficientemente motivada y documentada. El RGPD no contiene una obligación expresa de motivación de estas decisiones. Sin embargo, la AEPD entiende que esta exigencia constituye un criterio interpretativo razonablemente derivado de la garantía de independencia prevista en el artículo 38 del RGPD, de la interpretación amplia realizada por el TJUE en la sentencia Leistritz respecto de las medidas desfavorables, de la protección reforzada prevista en el artículo 36.2 LOPDGDD y de las exigencias generales de responsabilidad proactiva y rendición de cuentas que inspiran el sistema europeo de protección de datos.

Este criterio encuentra además apoyo en el Informe Jurídico AEPD 0038/2023, así como en las orientaciones de las autoridades irlandesa y finlandesa, que insisten en la necesidad de documentar las razones por las que la organización decide apartarse del criterio expresado por el DPD.

Por ello, cuando una organización adopte decisiones que afecten al nombramiento, permanencia, funciones, recursos o posición institucional del DPD, resulta recomendable que deje constancia expresa de las razones que justifican dichas decisiones.

Esta práctica favorece la transparencia, facilita el control posterior de legalidad y contribuye a reforzar la confianza en la independencia de la función.

G. PROTECCIÓN FRENTE A MEDIDAS ORGANIZATIVAS QUE AFECTEN MATERIALMENTE A LA INDEPENDENCIA DEL DPD

La protección de la independencia del DPD reconocida por el artículo 38.3 del RGPD no debe analizarse exclusivamente desde la perspectiva del cese formal. La interpretación amplia realizada por el TJUE en la sentencia Leistritz, el criterio sostenido por la AEPD en su Informe Jurídico 0038/2023, los resultados de la Coordinated Enforcement Action del CEPD sobre designación y posición del DPO y las orientaciones neerlandesas sobre la posición institucional del FG permiten sostener que determinadas medidas

organizativas pueden comprometer la independencia del DPD aun cuando no impliquen formalmente su destitución.

No existe actualmente una categoría jurídica consolidada de "remoción encubierta" o "destitución material". Sin embargo, sí puede afirmarse que determinadas decisiones organizativas deben examinarse especialmente a la luz de las garantías de independencia previstas por los artículos 38.1, 38.2 y 38.3 RGPD. Entre ellas pueden encontrarse:

- la retirada sustancial de funciones propias del DPD;
- la pérdida de acceso directo a la alta dirección;
- la reducción significativa de recursos indispensables para el desempeño de sus funciones;
- la supresión de estructuras de apoyo necesarias para el ejercicio efectivo de la función;
- la reasignación de competencias esenciales a otros órganos;
- cualquier otra medida que vacíe sustancialmente de contenido las funciones atribuidas al DPD.

En estos supuestos, las organizaciones deberían evaluar expresamente el impacto de la medida sobre la independencia y capacidad de actuación del DPD y documentar las razones que justifican su adopción.

H. PROTECCIÓN FRENTE A REPRESALIAS Y GARANTÍAS ORGANIZATIVAS MÍNIMAS

La independencia del DPD exige una protección efectiva no solo frente a su destitución o sanción por el desempeño de las funciones que le atribuye el RGPD, sino también frente a otras decisiones desfavorables que constituyan una reacción a su ejercicio legítimo. Esta interpretación encuentra apoyo en el artículo 38.3 RGPD, en la sentencia Leistritz (C-534/20) y en las Directrices WP243 rev.01 del Grupo de Trabajo del Artículo 29, asumidas por el CEPD.

La Autoridad de Protección de Datos belga concreta especialmente esta garantía en sus orientaciones sobre independencia del DPD, actualizadas el 24 de enero de 2024. Explica que la protección comprende medidas perjudiciales para su carrera profesional, como retrasos en la promoción, denegación de ventajas o amenazas de adoptar decisiones desfavorables por el ejercicio de sus funciones. Se trata de una protección frente a represalias, no de una prohibición general de adoptar decisiones laborales legítimas por causas ajenas a su actividad como DPD.

A su vez, el Informe del CEPD sobre la acción coordinada relativa a la designación y posición de los DPD, adoptado en enero de 2024, identifica en su apartado 4.5.2 las injerencias derivadas de instrucciones, relaciones contractuales o dependencia

presupuestaria. Entre sus recomendaciones figuran la formalización de las condiciones de ejercicio de la función y la posibilidad de conservar evidencias de las interferencias sufridas.

Estas orientaciones, junto con las garantías de recursos, autonomía y reporte directo previstas en el artículo 38 RGPD, justifican recomendar que las organizaciones adopten medidas organizativas capaces de prevenir las represalias y asegurar que el DPD pueda desarrollar sus funciones de forma efectiva e independiente. Las orientaciones de la CNIL francesa y de las autoridades danesa y sueca sobre independencia del DPD ofrecen respaldo institucional complementario a este planteamiento.

Para garantizar la efectividad de esta protección, las organizaciones deberían, al menos, asegurar de manera estable:

- acceso directo al más alto nivel de dirección;
- recursos humanos y materiales suficientes;
- acceso a la información necesaria para el desempeño de sus funciones;
- apoyo organizativo adecuado;
- formación continua;
- capacidad real para elevar riesgos, observaciones y discrepancias a los órganos competentes.

Estas garantías organizativas no constituyen elementos accesorios, sino condiciones indispensables para preservar la independencia efectiva del DPD y asegurar el correcto funcionamiento del sistema de cumplimiento en materia de protección de datos.

VI. EL DPD Y LA SUPERVISIÓN DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

Algunas de las obligaciones que implícitamente asigna el RGPD al responsable, con la implicación del DPD en tiempo y forma, no suponen un conflicto de intereses en la medida en que no exista un poder decisorio del DPD sobre las decisiones finales que pueda adoptar el responsable del tratamiento en relación con los fines y medios del tratamiento.

Existirá un conflicto de intereses manifiesto cuando el DPD ocupe posiciones que le permitan determinar, o influir de forma determinante en, los fines y medios del tratamiento de datos personales.

Dado que la definición de dichos fines y medios es competencia exclusiva del responsable del tratamiento, el DPD no podrá desempeñar cargos operativos o decisorios que deban ser objeto de su propia supervisión.

A. POLÍTICAS DE PROTECCIÓN DE DATOS

En ocasiones**,** puede ocurrir que el responsable o el encargado del tratamiento desarrollen políticas de protección de datos para dar cumplimiento a lo previsto en el artículo 24 del RGPD sin el asesoramiento del DPD y sin considerar posibles conflictos de intereses de la organización. En este sentido, dado el conocimiento que el DPD tiene de la organización, sus procesos y sus operaciones de tratamiento, resulta esencial su asesoramiento al responsable para que este tome la decisión de abordar el desarrollo de las políticas de protección de datos a las que se refiere el artículo 24 del RGPD, sobre las que el DPD posteriormente desempeñará su función de supervisión. En este ámbito, el DPD es una garantía para el funcionamiento institucional o corporativo a la hora de desarrollar políticas que supongan una mejora para el funcionamiento general y la confianza de terceros en la organización.

Como se ha señalado, el DPD puede asesorar al responsable o al encargado en la evaluación de la necesidad de desarrollar políticas de protección de datos; puede también participar asesorando al responsable y al encargado en su desarrollo, y será posteriormente el encargado de supervisar su aplicación y sus carencias para sugerir al responsable posibles mejoras.

Para poder demostrar que el DPD ha sido tenido en cuenta en tiempo y forma, el responsable o el encargado deben disponer de medios para acreditar que se ha recabado su asesoramiento. Estos medios señalarán también aquellos aspectos en los que el responsable o el encargado no han asumido las recomendaciones del DPD, con una clara exposición de los motivos. Una manera de acreditar el asesoramiento del DPD es la elaboración de informes por parte de este, como se señala en el WP243, en los que se incluya un extracto de las acciones de asesoramiento y supervisión realizadas, con el detalle de las comunicaciones dirigidas al responsable con fines de asesoramiento y supervisión.

Además del papel de asesoramiento al responsable, el artículo 39 del RGPD exige que el DPD ejerza su función de supervisión sobre dichas políticas[18], incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, así como las auditorías que correspondan en cada caso.

Un responsable que diera instrucciones al DPD para que elabore, apruebe o actualice una política de protección de datos que debe supervisar el propio DPD estaría vulnerando el principio de independencia del DPD y generando un conflicto de intereses en el desarrollo de su labor. La política de protección de datos debe incluir de manera ejecutiva y efectiva mecanismos que demuestren que el responsable cuenta con el DPD

[18] Art. 39 apartado 1 letra b) entre las funciones mínimas del DPD establece que *debe 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.*

y recibe su asesoramiento. Sin embargo, es el propio responsable quien debe establecer estos mecanismos[19] y la forma en que se lleven a cabo dentro de la organización. Estos mecanismos serán supervisados por el DPD en las correspondientes auditorías de protección de datos o cuando fuera necesario.

B. ELABORACIÓN Y MANTENIMIENTO ACTUALIZADO DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO (RAT) Y DEL INVENTARIO DE ACTIVIDADES DE TRATAMIENTO

El artículo 30 del RGPD obliga al responsable y al encargado a mantener un registro actualizado de sus actividades de tratamiento. Este registro no es un mero trámite formal, sino una herramienta dinámica y esencial del principio de responsabilidad proactiva.

Una gestión deficiente del RAT implica la pérdida de control operativo, lo que deriva en riesgos críticos de cumplimiento: falta de transparencia, evaluaciones de impacto (EIPD) y análisis de riesgos deficientes o inexistentes, fallos en la privacidad desde el diseño y por defecto, etc. Más allá del mínimo legal, el DPD puede incluir información y datos clave para la adecuada y necesaria gestión técnica y organizativa que supongan mejoras operativas en la gestión de los tratamientos, tales como:

- Unidad orgánica gestora de la información y personas de contacto.
- Información relativa a los sistemas de información necesarios para las operaciones de tratamiento y personas de contacto:
  - Identidad de los responsables de los sistemas de información
  - Datos de contacto de los responsables de los sistemas de información
  - Información operativa en casos de brechas de datos
- Datos de contacto de la unidad de seguridad del sistema de información o del responsable de seguridad de la información.
- Procedimiento general para la toma de acciones en caso de brechas de seguridad.
- Información relativa a los encargados del tratamiento
- Procedimiento de modificación de las operaciones de tratamiento y su incorporación al registro de actividades de tratamiento.
- etc.

En definitiva, el RAT es una herramienta de trabajo que constituye el punto de partida esencial para la descripción documental de las actividades y operaciones de

[19] Guía para la "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales": *El gobierno o gobernanza de datos es el proceso por el que se implementan políticas y procedimientos para garantizar una gestión efectiva y eficiente de la información en la entidad. Estas políticas se proyectan en la gestión de cada tratamiento específico.*

tratamiento, lo que posibilita el resto de las acciones de cumplimiento que puedan ser necesarias en función de cada caso.

Por otra parte, a la vista de lo señalado y del conocimiento que el DPD tiene de la organización, su implicación material en la gestión del RAT le permite identificar detalles de las operaciones de tratamiento que van más allá del mero cumplimiento formal de los artículos 30 del RGPD y 31 de la LOPDGDD. Por ejemplo, le permitirá relacionar las operaciones de tratamiento con el uso de agentes y asistentes de IA en los procesos de la organización, aspecto necesario para definir el riesgo inherente de las operaciones de tratamiento y las consiguientes obligaciones de cumplimiento normativo del responsable, sobre las que el DPD ejercerá sus funciones de supervisión, como las EIPD.

Teniendo en cuenta que el RAT debe estar a disposición de la autoridad de control (art. 30.4 RGPD) y que el DPD es el punto de contacto entre el responsable y la autoridad de control, sería posible que el responsable o el encargado, en su política de protección de datos, delegara la gestión del registro de actividades de tratamiento como parte de la función de supervisión del DPD[20]. En esta función de supervisión y auditoría**,** el DPD verifica la puesta en marcha de nuevos tratamientos y operaciones de tratamiento**,** llevando a cabo procesos de auditoría para detectar posibles operaciones de tratamiento implementadas al margen de los procedimientos establecidos, con el objetivo de garantizar el control efectivo de las operaciones de tratamiento por parte del responsable.

Lógicamente, partiendo de la información contenida en el RAT, es también posible que el responsable delegue en el DPD el mantenimiento y actualización del inventario de actividades de tratamiento (art. 31 LOPDGDD) para los sujetos obligados[21] o para aquellos responsables o encargados que, no siendo sujetos obligados, deseen utilizar este mecanismo de transparencia de manera voluntaria.

En cualquier caso, el DPD no dispone de poder decisorio para implementar nuevas operaciones de tratamiento o nuevos tratamientos. Corresponde al responsable acreditar que el criterio del DPD fue tenido en cuenta antes de aprobar y poner en marcha nuevas operaciones o actividades de tratamiento.

La política de protección de datos de la organización podría implicar materialmente al DPD en los procesos relacionados con la llevanza del registro de actividades de tratamiento, estableciendo la obligación de recabar su asesoramiento y definiendo las actividades de supervisión del DPD relacionadas con el RAT, siempre que su implicación

[20] WP243: 4.5. Papel del DPD en el mantenimiento de registros
En cuanto a los registros de las actividades de tratamiento, es obligación del responsable o del encargado del tratamiento, y no del DPD, mantener los registros de las operaciones de tratamiento. No obstante, nada impide que el responsable o el encargado del tratamiento asignen al DPD la tarea de mantener un registro de las operaciones de tratamiento bajo la responsabilidad del responsable o del encargado del tratamiento. Dicho registro debe considerarse una de las herramientas que permiten al DPD realizar sus funciones de supervisión de la observancia de la normativa y de información y asesoramiento al responsable o al encargado del tratamiento.
[21] Art. 77 apartado 1 LOPDGDD

no suponga la toma de decisiones sobre los fines y medios del tratamiento o de una operación de tratamiento determinada.

C. EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS (EIPD)

Sobre la base de una adecuada gobernanza del registro de actividades de tratamiento, podrá abordarse la gestión del riesgo para los derechos y libertades de las personas físicas y, en su caso, el asesoramiento del DPD en materia de dichos riesgos señalará al responsable la obligación, la necesidad o la recomendación de realizar una evaluación de impacto en protección de datos sobre un tratamiento o una operación de tratamiento.

Asimismo, la política de protección de datos puede establecer los términos de la implicación del DPD desde la fase del desarrollo conceptual de una nueva actividad de tratamiento o de una nueva operación de tratamiento, así como los objetivos de dicha implicación. Entre estos objetivos puede tenerse en cuenta que el DPD asesore al responsable en la descripción de las operaciones de tratamiento, su riesgo inherente, la metodología a utilizar para la gestión del riesgo o la EIPD, las medidas de diseño y por defecto, las medidas de seguridad, la conveniencia de externalizar la EIPD o la necesidad de proponer al responsable la modificación del concepto inicial del tratamiento o de las operaciones de tratamiento.

Finalmente, el DPD puede asesorar al responsable en la valoración final de la EIPD y, si el riesgo residual fuera elevado[22], asesorarle y proponerle consultar[23] a la autoridad de control mediante el mecanismo de consulta previa que establece el artículo 36 del RGPD. Como punto de contacto con la autoridad de control[24], el DPD también podrá solicitar materialmente el asesoramiento de la autoridad de control sobre el riesgo de las operaciones de tratamiento.

En definitiva, el responsable y el encargado del tratamiento deberán contar con la participación del DPD en la identificación de los riesgos y su evaluación, en la identificación de medidas de diseño, y de minimización, en la propuesta de los requisitos de seguridad para los tratamientos y las operaciones de tratamiento, o en cualquier otra cuestión que, dentro de su asesoramiento, pudiera suponer una mejora para la protección de los derechos y libertades de las personas físicas. Como en cualquier otro caso de desacuerdo o discrepancia entre el asesoramiento del DPD y las decisiones del

[22] Guía para la "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales: *El proceso de consulta previa tiene como objeto presentar ante la Autoridad de Control un tratamiento que sea conforme con el RGPD, que tenga obligación o se haya valorado la oportunidad, o conveniencia, de realizar una EIPD, pero que entrañe un nivel de riesgo residual para los derechos y libertades de los ciudadanos que podría resultar inaceptable.*

[23] Art. 39 RGPD en su apartado primero letra e) establece como una de las funciones del DPD la de 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.

[24] El Art. 39 RGPD apartado primero letra e) entre las funciones mínimas que debe realizar el DPD incluye la de *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.*

responsable, se deberá dejar constancia de la situación y de los motivos por los que el responsable ha adoptado una decisión contraria a la opinión del DPD.

En ningún caso el DPD aprueba o asume la decisión final de continuar con un tratamiento o sobre las salvaguardas a aplicar; esas decisiones corresponden al responsable del tratamiento, aunque con el asesoramiento del DPD.

Un caso particular de asesoramiento al responsable en el ámbito de las Administraciones Públicas es el que debe existir con ocasión del desarrollo de proyectos normativos. En este caso, el asesoramiento del DPD es clave a la hora de identificar medidas normativas que pudieran no ser necesarias ni proporcionadas o no ajustarse al derecho de un Estado miembro o al Derecho en general[25]. En estos supuestos, es esencial la participación del DPD para garantizar que la medida legislativa respete los principios de necesidad y proporcionalidad en aquellos casos en los que dicha medida implique, en general, una reducción de los derechos y libertades de las personas físicas, incluso cuando inicialmente no fuera posible identificar las operaciones de tratamiento que dicha medida pudiera finalmente implicar.

Una política que atribuya al DPD la responsabilidad de realizar o aprobar la EIPD, gestionar los riesgos para los derechos y libertades o adoptar la decisión final sobre las medidas de protección de datos desde el diseño y por defecto o las medidas de seguridad podría generar un conflicto de intereses, al situarle en la posición de supervisar posteriormente decisiones o actuaciones de las que él mismo fuera responsable.

D. BRECHAS DE SEGURIDAD

El asesoramiento del DPD al responsable y al encargado del tratamiento en materia de riesgos para los derechos y libertades de las personas físicas debe incluir los riesgos que una brecha de datos personales puede suponer para los interesados, tal y como exige el artículo 32 del RGPD[26]. La política de protección de datos puede establecer los mecanismos para garantizar este asesoramiento y el reporte al responsable, de modo que se acredite la existencia del asesoramiento y la supervisión del DPD cuando se produce una brecha de datos personales.

Asimismo, la política de protección de datos puede establecer la implicación material del DPD en los procesos de notificación (art. 33 RGPD) a la autoridad de control y en los procesos de comunicación a los interesados (art. 34 RGPD), teniendo en cuenta que el artículo 39 del RGPD establece entre las funciones del DPD la de cooperar con la autoridad de control y la de actuar como punto de contacto de esta para cuestiones

[25] Guía de "Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo"
[26] Artículo 32 RGPD apartado 2: *Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.*

relativas al tratamiento[27], como es el caso de la notificación de brechas de datos personales a la autoridad de control.

Como resultado del asesoramiento del DPD al responsable o al encargado del tratamiento en materia de brechas de datos personales, se podrán elaborar notas e informes técnicos internos en relación con las medidas de diseño, las medidas por defecto, las medidas de seguridad o cualquier otro aspecto relacionado con las brechas de datos personales que tuvieran lugar en la organización. Estas notas podrán ser aprobadas o rechazadas por el responsable, que dejará constancia de dicha aprobación o discrepancia.

Este asesoramiento y supervisión del DPD en la gestión de brechas no debe confundirse con la responsabilidad operativa en la gestión del incidente, que corresponde a las áreas técnicas y a los responsables competentes.

Una política de protección de datos no puede delegar en el DPD la responsabilidad y la toma de decisiones relacionadas con una brecha de datos personales que directa o indirectamente impliquen poder decisorio sobre los fines y medios del tratamiento.

E. AUDITORÍAS DE PROTECCIÓN DE DATOS

Las funciones de asesoramiento y supervisión del DPD incluyen la revisión de la eficaz implementación de las medidas y su actualización cuando sea necesario[28], lo que en la práctica se traduce en reportar al responsable la necesidad de modificar o actualizar las medidas y en participar en los procesos de auditoría de protección de datos encaminados a garantizar el cumplimiento de la normativa de protección de datos, dotando al DPD de capacidad de inspección e investigación en la organización. La participación del DPD es un elemento esencial para garantizar el cumplimiento de la normativa de protección de datos y el artículo 39 del RGPD asigna explícitamente la función de participar en las auditorías que pudieran ser necesarias para supervisar el cumplimiento tanto de lo dispuesto en el RGPD como de lo dispuesto en las políticas de protección de datos del responsable o el encargado del tratamiento.

Uno de los motivos habituales por los que el DPD puede reportar al responsable la necesidad de realizar cambios en un tratamiento o en una operación de tratamiento, o de proponer nuevas medidas técnicas y organizativas, son las brechas de datos personales. Cuando se produce una brecha**,** es necesario revisar la evaluación inicial del

[27] Artículo 39 RGPD apartado 1 d) y e) funciones del DPD:
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.

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

riesgo y evaluar la eficacia de las medidas existentes o la necesidad de implantar medidas adicionales (medidas de diseño, medidas de minimización de datos, medidas de anonimización, medidas criptográficas, medidas de seguridad, etc.) que permitan evitar o mitigar el riesgo o los riesgos derivados de la brecha de datos personales. En ocasiones, el DPD, como resultado de una brecha de datos personales y en el ejercicio de sus funciones de asesoramiento y supervisión en materia de riesgos para los derechos y libertades de las personas físicas, puede proponer al responsable llevar a cabo una auditoría relativa a un tratamiento o a una operación de tratamiento, o bien una auditoría de protección de datos de toda la organización.

VII. SITUACIONES QUE REQUIEREN UNA EVALUACIÓN ESPECÍFICA DE LA INDEPENDENCIA DEL DPD

Con carácter general, la compatibilidad entre las funciones del DPD y otros puestos o responsabilidades no puede determinarse exclusivamente atendiendo a la denominación formal del cargo. Debe analizarse caso por caso, considerando las funciones efectivamente ejercidas, la capacidad de decisión asociada al puesto y la estructura organizativa concreta.

Sin embargo, podrá existir un conflicto de intereses cuando las funciones adicionales permitan al DPD determinar, aprobar o influir de manera decisiva en los fines y medios de tratamientos que posteriormente deba supervisar. La mera participación en funciones de asesoramiento, apoyo, coordinación o verificación no implica necesariamente la existencia de un conflicto, siempre que el DPD no asuma la decisión final ni supervise sus propias actuaciones ni reciba instrucciones que comprometan su independencia. No obstante, existen circunstancias en las que la naturaleza de las funciones y responsabilidades que asumiera un DPD podrían generar un conflicto de intereses en el ejercicio de sus funciones.

En todo caso, el responsable o el encargado debe valorar y graduar los riesgos de conflicto de intereses de aquellas situaciones que puedan incidir en su independencia; de forma general, en aquellas situaciones en las que el DPD pueda decidir en distinta medida los fines y medios del tratamiento o que, sin decidir sobre estos, pueda afectar a su implantación o despliegue, más allá de las labores que como DPD le corresponden. Una vez valorados los riesgos de conflicto de intereses, deberá identificar las medidas idóneas que permitan mitigar dichos riesgos, tales como la segregación funcional, la validación independiente por un tercero o la abstención reglada. Tanto el procedimiento como la valoración del riesgo potencial y residual una vez aplicadas las medidas deben quedar suficientemente documentados.

Este apartado proporciona orientaciones que pueden tenerse en cuenta a la hora de identificar posibles riesgos de conflicto de intereses en la ejecución de actividades del DPD a efectos de que el responsable o encargado, según corresponda, identifique los

riesgos de conflicto y, en su caso, identifique e implante medidas que efectivamente reduzcan o eviten esos riesgos. Por tanto, las posiciones y situaciones examinadas en este apartado tienen carácter orientativo y no constituyen una relación de incompatibilidades automáticas o estructurales, sino supuestos que habrá que analizar en función de la efectividad de las medidas de mitigación.

A. EL DPD EN LOS PROCESOS DE CONTRATACIÓN

La participación del DPD en los procesos de contratación de manera temprana es necesaria para determinar requisitos de diseño y funcionalidades que, por defecto, resulten menos intrusivas para los interesados o, en general, que impliquen un menor riesgo para los derechos y libertades de las personas físicas.

Sin embargo, además de los contratos, existen otros vínculos jurídicos (protocolos, convenios, acuerdos, etc.) en los que implícitamente puede haber operaciones o tratamientos de datos personales y en cuya elaboración también es necesaria la participación del DPD, y no exclusivamente en la revisión de los términos que exige el artículo 28 del RGPD sino en todo lo relativo al cumplimiento general de la normativa de protección de datos.

La contratación de un producto o de un servicio cuyos procesos incluyen datos personales precisa el asesoramiento del DPD al responsable, en tiempo y forma, tanto para la adquisición de los productos o servicios que puedan resultar más idóneos desde el punto de vista de la protección de los derechos y libertades de las personas físicas como para garantizar la minimización en su configuración.

El asesoramiento del DPD puede abarcar aspectos como la gestión de flujos internacionales de datos (capítulo V del RGPD), el seguimiento y revisión de la relación contractual (art. 28 RGPD) o el asesoramiento al responsable en relación con la obligación de diligencia en la selección de terceros implicados en el tratamiento. En este sentido, el responsable y el encargado deberían recabar la opinión del DPD con carácter previo al desarrollo de requisitos de productos y servicios y a su contratación, cuestión que podría incluirse en la política de protección de datos del responsable. Finalmente, tras la contratación de un producto o servicio, el DPD asesorará al responsable en el desarrollo y configuración por defecto de dicho producto o servicio y llevará a cabo las auditorías que permitan al responsable demostrar el cumplimiento de lo previsto en el RGPD.

En ningún caso corresponde al DPD decidir la adquisición de un producto o un servicio, tomar decisiones relacionadas con la configuración de dicho producto o servicio ni asumir la representación del responsable en los procesos de adquisición de productos o servicios.

Un DPD que trabaja en el departamento de contrataciones y representa al responsable en los procesos de contratación estaría tomando decisiones sobre aquellas licitaciones o contrataciones que implican un posible encargo de tratamiento de datos personales,

ya fuera en su posición de contratante o de contratado. Si el DPD participara con poder decisorio en la contratación o en la negociación de pliegos, existe un riesgo de que se produzca un conflicto de intereses pues podría terminar supervisando sus propias decisiones.

Un DPD que participa con el departamento TIC en la configuración por defecto de las plataformas y en la toma de decisiones relacionadas con la información que dichas plataformas van a recopilar sobre las personas físicas o el tiempo de retención de los datos de los logs, estaría tomando decisiones de configuración de los sistemas que él mismo deberá supervisar en el futuro, lo que contravendría la obligación de independencia y objetividad requerida por la norma y generaría un riesgo de conflicto de intereses**.**

B. DPD CON OTROS ROLES Y RESPONSABILIDADES EN LA ORGANIZACIÓN

El artículo 38 del RGPD, en su apartado sexto[29], permite al DPD desempeñar otros cometidos. En tal caso, el responsable o encargado del tratamiento velará por que su ubicación jerárquica y responsabilidades adicionales no generen conflictos de intereses que menoscaben su autonomía técnica e independencia funcional.

Los aspectos que evidencian posibles conflictos de intereses para un DPD están directamente relacionados con su independencia funcional. En este sentido, la regla práctica principal es que si un rol dentro de la organización, directa o indirectamente, define, participa o aprueba los fines y medios del tratamiento de datos personales, esta tarea excluye su designación como DPD.

La determinación de un conflicto de intereses debe realizarse caso a caso, considerando la estructura organizativa específica de cada organización y todas las normativas que le sean aplicables.

A continuación, se señalan algunos ejemplos de puestos y situaciones que habitualmente pueden dar lugar a conflictos de intereses y, por tanto, a su incompatibilidad.

1. Cargos de alta dirección con funciones operativas de decisión sobre explotación de datos

El Comité Europeo de Protección de Datos**,** en sus Directrices WP243, ha señalado que puestos como el de director general, director de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI se consideran, por regla general, incompatibles con la función del DPD. La combinación de la función de DPD con puestos de alta dirección requiere una cautela particular por parte de las organizaciones. Incluso cargos inferiores

[29] **Artículo 38 RGPD**:
6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

en la estructura organizativa pueden generar conflicto si implican, directa o indirectamente, la determinación de los fines y medios del tratamiento.

Los responsables de Tecnologías de la Información y las Comunicaciones (TIC), o posiciones similares, tampoco pueden ocupar el puesto de DPD en la medida en que sus funciones implican decisiones sobre la existencia del tratamiento, el modo de tratar los datos, o decisiones sobre la configuración de sistemas, productos o servicios que posteriormente deberán supervisar como DPD. El DPD actúa como asesor y supervisor interno, no como una figura que toma decisiones sobre el tratamiento de datos.

Los cargos de alta dirección, como el de responsable del departamento de mercadotecnia, se consideran en conflicto con la figura del DPD, dado que sus funciones implican la toma de decisiones relacionadas con la determinación de los fines y medios del tratamiento de datos personales para, por ejemplo, campañas, desarrollo de productos, gestión de clientes, investigación de mercado, perfilado de personas, etc.

El responsable de recursos humanos es otro puesto de alta dirección que se considera en conflicto, dado que su función implica la toma de decisiones sobre el tratamiento de datos personales de los empleados y de otras personas con intereses vinculados a las relaciones laborales. Desde la dirección de recursos humanos se gestionan datos personales de empleados y se toman decisiones sobre los procesos y las herramientas con las que se tratan los datos, lo que significaría que el DPD estaría supervisando estas decisiones desde un claro conflicto de intereses. Esta situación no es exclusiva del responsable de recursos humanos de una organización: también personas de nivel inferior en la organización pueden estar involucradas, directa o indirectamente, en la toma de decisiones relacionadas con los datos de los trabajadores o en la configuración y selección de plataformas y sistemas para la gestión de los datos personales de los empleados.

En general, pueden resultar incompatibles con el desempeño de la labor de DPD los responsables de departamentos y unidades que decidan sobre datos, como los del padrón, la historia clínica, la videovigilancia, el pago de tributos, etc., incluso cuando ocupen cargos inferiores a los de la alta dirección, siempre que sus funciones lleven a la determinación de los fines y medios del tratamiento de datos personales, les permitan influir directamente sobre la determinación de dichos medios y fines o los involucren, directa o indirectamente, en esta toma de decisiones. Esto incluiría, por ejemplo, a los responsables de unidades que toman decisiones sobre bases de datos sensibles o de gran volumen en el sector público.

2. Responsable de seguridad de la información (CISO/RSI) si decide medidas, herramientas o niveles de seguridad

La figura del DPD debe diferenciarse de la del Responsable de Seguridad de la Información (RSI o CISO), figura regulada en el Real Decreto 43/2021, de 26 de enero y mencionado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema

Nacional de Seguridad. El RSI puede tomar decisiones relativas a los tratamientos de datos con fines de seguridad o recibir instrucciones directas del responsable de la información, mientras que el RGPD exige que el DPD no reciba instrucciones del responsable del tratamiento o del responsable de la información en el desempeño de sus funciones.

El DPD asesora al responsable en las evaluaciones de impacto y en cualquier otro aspecto del tratamiento, pero es el responsable quien adopta las decisiones finales sobre los fines, medios y salvaguardas que pudieran ser necesarias para garantizar los derechos y libertades y proteger los intereses de las personas físicas. El RSI garantiza la seguridad de la información y del sistema de información, mientras que el DPD asesora sobre los requisitos de seguridad que puedan resultar necesarios para garantizar la protección de los derechos y libertades de las personas en cuanto al tratamiento de sus datos.

Asignar al DPD responsabilidades directas en un ámbito que este debe supervisar, y en el que estaría sujeto a instrucciones de otros órganos, impide su independencia y genera conflictos de intereses en su labor de supervisión.

Excepcionalmente, en organizaciones pequeñas con recursos limitados, la designación de la misma persona como DPD y RSI podría ser admisible, siempre y cuando se garanticen y documenten medidas organizativas que aseguren su autonomía, su independencia y la ausencia de conflictos de intereses[30]. Esta situación debe entenderse como coyuntural y debe resolverse tan pronto como sea posible. Sería el caso, por ejemplo, de un organismo de nueva creación que aún no ha sido dotado materialmente de los recursos necesarios para abordar separadamente la designación de ambos perfiles.

3. Responsable del canal ético y del canal del informante[31]

El responsable del canal ético y del canal del informante será la persona designada por el órgano obligado, que, en calidad de responsable del sistema, tomará decisiones relacionadas con la información personal tratada. Dado que el DPD debe prestar su función de asesoramiento y supervisión en los tratamientos de datos personales que tienen lugar en el ámbito de aplicación de la Ley 2/2023, la acumulación de ambas funciones le pondría en una evidente posición de conflicto de intereses, en la medida en que estaría supervisando sus propias decisiones como responsable del canal del informante o del canal ético.

Incluso cuando el responsable del canal interno de protección del informante (sistema interno de información) fuera un órgano colegiado del que formase parte el DPD, la organización deberá prever mecanismos para su abstención cuando el ejercicio de sus

[30] Informe jurídico 2018-0170

[31] Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

funciones pudiera dar lugar a un posible conflicto de intereses como DPD y responsable del canal. Idéntica solución se requeriría en los canales éticos de las organizaciones.

4. Chief Data Officer / Analítica de Datos / IA / Ciencia de Datos con poder para definir usos de datos y modelos

La rápida adopción de modelos de inteligencia artificial (IA) en las organizaciones exige que el DPD adquiera nuevas competencias que le permitan ejercer sus funciones desde las fases iniciales del diseño de los sistemas de IA o de explotación de datos, así como en la definición de casos de uso y modelos.

Esto plantea nuevos retos en la relación entre estos roles emergentes y el del DPD, sin que ello implique que este pueda tomar decisiones sobre los fines o medios de la IA ni sobre cualquier analítica de datos que deba supervisar en el desempeño de sus funciones.

El DPD no puede tomar decisiones que pudieran ser necesarias a la hora de seleccionar conjuntos de datos o de utilizar mecanismos de IA que puedan incluirse en los procesos de la organización; tampoco puede tomar decisiones en relación con cualquier fin secundario al que pudieran destinarse los datos recabados con una finalidad inicial distinta (*machine learning*, analítica de datos, etc.). Sin embargo, su asesoramiento y supervisión son factores clave para garantizar la confianza de los interesados, en especial, en relación con los posibles usos secundarios a los que pudieran destinarse los datos de las personas físicas.

Con carácter general, el DPD no asume la decisión final sobre los fines y medios de la IA o los usos de datos, pero puede y debe asesorar al responsable sobre la selección y adecuación de conjuntos de datos, su posible exceso, los mecanismos de IA, los usos secundarios y las posibles alternativas que podrían reducir el impacto sobre los derechos y libertades de las personas físicas.

C. POSICIONES EN LA ORGANIZACIÓN POTENCIALMENTE COMPATIBLES

Los puestos potencialmente compatibles con la función de DPD son aquellos que, por su naturaleza, se centran en el asesoramiento, la verificación o la auditoría, pero no tienen capacidad de decisión sobre los fines y los medios del tratamiento de datos personales.

La determinación de un posible conflicto de intereses que pudiera generarse por simultanear sus funciones con otras funciones de la organización debe realizarse caso a caso, considerando la estructura organizativa específica y todas las normativas aplicables. Los conflictos de intereses en estas posiciones podrían asumirse como evidentes, aparentes o potenciales de acuerdo con la terminología de la norma ISO; en la práctica, lo recomendable sería disponer de un DPD a tiempo completo y sumarle otras funciones cuando sea posible.

1. Asesoría jurídica / Cumplimiento normativo

La función de asesoramiento jurídico o de cumplimiento normativo es, de hecho, una de las áreas más comunes de especialización para un DPD. Su labor será compatible con aquella siempre que su intervención se limite a ofrecer asesoramiento, orientación y supervisión, sin participar en la aprobación o determinación de los fines y medios del tratamiento de datos personales.

La compatibilidad deberá analizarse atendiendo a las responsabilidades efectivamente asumidas. Podrá existir un conflicto de intereses cuando la persona designada como DPD adopte decisiones operativas sobre tratamientos que posteriormente deba supervisar o cuando se le encomiende la representación o defensa de la organización en asuntos en los que deba mantener una posición independiente como DPD.

Cuando se solicita al DPD que represente al responsable o encargado del tratamiento ante los tribunales o en procedimientos de infracción en materia de protección de datos**,** se genera un conflicto de intereses, ya que ello implica asumir la defensa de la organización, es decir, velar por los intereses de la organización, lo que dificulta la neutralidad de su función de supervisión y asesoramiento.

2. Auditoría interna / Gestión de riesgos / Calidad

La auditoría interna o la gestión de riesgos se desarrollan por roles que evalúan y recomiendan, pero, al igual que el DPD, no toman las decisiones finales sobre la implementación de las medidas, los fines o los medios del tratamiento o la configuración de sistemas o dispositivos, como ocurre en el caso de una EIPD. Un responsable o un encargado lo siguen siendo con independencia de este asesoramiento y supervisión en relación con el cumplimiento del RGPD.

Cuando el ámbito o el alcance de una auditoría va más allá de las funciones del DPD, la independencia de sus funciones podría verse comprometida.

Un conflicto de intereses surgiría si el DPD participara en la gestión de riesgos financieros y tomara decisiones sobre la capacidad económica de los interesados, o si interviniera en una auditoría o investigación de mercado que implique analizar y seleccionar potenciales clientes según determinados perfiles de consumidor, con el fin de generar dichos perfiles.

3. Transparencia, archivo y gobierno del dato

El DPD contribuye a la transparencia con relación a los tratamientos de datos personales. Con este objetivo, sus funciones de supervisión pueden requerir la recopilación de información para identificar actividades de tratamiento y el análisis y verificación del cumplimiento normativo. Estos roles son compatibles siempre que el DPD no tenga poder de decisión sobre la forma en que los datos se archivan, gestionan o utilizan. Es decir, que su función sea únicamente acceder a los datos con fines de supervisión y asesoramiento para asegurar que estas actividades cumplan con el RGPD.

Cuando el acceso a datos personales implica la toma de decisiones en procesos de negocio con objetivos como administrar los datos, implementar medidas de seguridad o modificar el ciclo de vida de los datos, diseñar un sistema de almacenamiento, etc., el DPD estaría tomando decisiones sobre los fines y medios del tratamiento y ejerciendo su función desde un conflicto de intereses; es decir, tendría que supervisar sus propias actividades con relación al gobierno del dato.

4. Inspecciones de servicio y DPD

La inspección de servicio de una institución es un proceso de supervisión y control para verificar el correcto funcionamiento de sus funciones, normas y procedimientos. En la medida en que el ejercicio de las funciones de la inspección de servicio pudiera implicar la toma de decisiones sobre los fines y medios del tratamiento de las informaciones recopiladas en su labor de inspección, su posterior supervisión por parte del mismo inspector o inspectora de servicio en calidad de DPD plantearía la existencia de un conflicto de intereses y podría comprometer la imparcialidad de su función de supervisión.

La adopción de protocolos de abstención en caso de conflicto de intereses permitiría la compatibilidad de ambas funciones.

D. ALGUNAS SITUACIONES QUE PODRÍAN COMPROMETER LA INDEPENDENCIA DEL DPD O FAVORECER LA EXISTENCIA DE POSIBLES CONFLICTOS DE INTERESES

1. Acceso a información sensible[32] o confidencial como DPD

Aunque el acceso a la información sensible o confidencial no constituye automáticamente un conflicto de intereses, cuando el DPD ejerce otros roles o funciones dentro de la organización, este acceso a información sensible podría generar un posible conflicto de intereses. Este podría ser el caso cuando el DPD tiene acceso a información de carácter reservado o clasificada. La evaluación del conflicto de intereses debe centrarse en si la concurrencia de funciones del DPD genera un conflicto real, potencial o aparente, y en las medidas para gestionar estos posibles conflictos.

2. Actuar como encargado del tratamiento

Cuando el encargado del tratamiento o un subencargado actúa al mismo tiempo en calidad de DPD, estaría supervisando y asesorando sobre sus propias actividades de tratamiento como encargado o subencargado, lo que daría lugar a un evidente conflicto de intereses que puede comprometer su independencia y autonomía como DPD.

Esta situación se podría producir cuando se subcontrata un producto o servicio que incluye, además, la prestación de funciones de DPD. Si la misma entidad que suministra

[32] Información sensible: cualquier información clasificada, información relativa al canal del informante, información sobre procedimiento sancionador, procedimientos penales, información reservada, información personal, información relativa al secreto industrial, información relativa a la inteligencia nacional o de negocio, etc.

el producto o servicio actúa como DPD y supervisa y asesora sobre sus propias actividades de tratamiento como encargado o subencargado**,** su asesoramiento y supervisión carecerían de valor, pues podría suponer una situación evidente de conflicto de intereses.

3. Representación legal o defensa de la organización

La atribución de la tarea de presentar alegaciones en defensa de la organización en procedimientos administrativos, civiles, laborales o penales en los que se produzca un tratamiento de datos personales se considera una injerencia en las funciones del DPD, ya que le exige asumir una función que se desvía de su misión de supervisión y asesoramiento, lo que comprometería su neutralidad e imparcialidad.

Esto mismo se puede producir si se solicita al DPD representar al responsable o encargado del tratamiento ante los tribunales o presentar alegaciones en un procedimiento de infracción, un apercibimiento o un procedimiento de derechos iniciado a instancias de una autoridad de control en protección de datos.

Con carácter general, cuando el DPD representa al responsable o al encargado podría plantearse un evidente conflicto de intereses en la medida en que no puede realizar su función crítica de supervisión con relación a los tratamientos de datos personales si al mismo tiempo tiene que defender otros intereses del responsable.

4. Multiplicidad de funciones y recursos insuficientes

Aunque el RGPD permite al DPD desempeñar otras funciones, se requiere que estas no generen un conflicto de intereses. La capacidad del DPD para asumir todas las funciones en las que se vea implicado es limitada, y esta incapacidad material o la falta de conocimientos para tomar decisiones en diferentes ámbitos puede afectar negativamente a sus funciones como DPD. Por ejemplo, cuando un DPD asume múltiples funciones adicionales, especialmente en varios departamentos, como los de auditoría, riesgo y cumplimiento, hay una alta probabilidad de que se produzca un conflicto de intereses, no solo por la posición en la que se encuentra**,** sino también por el gran volumen de cometidos que debe afrontar.

La multiplicidad de funciones puede dar lugar al abandono total o parcial de sus funciones como DPD o a que priorice sus funciones en función de intereses propios o de terceros.

En aquellos casos en los que el DPD debe atender a un elevado número de responsables y encargados de manera simultánea el riesgo de incurrir en un conflicto de intereses es elevado que se multiplica cuando la atención a múltiples responsables y encargados se realiza mediante costes anormalmente bajos que podrían significar que el licitador no estuviera en condiciones de ejecutar correctamente su labor de DPD por el precio ofertado y, en consecuencia, por la falta de recursos económicos de los que debería disponer. En estos casos, se deberá justificar debidamente la viabilidad de una determinada oferta, en especial, en el caso de las administraciones públicas.

5. DPD a tiempo parcial o compartido

Los DPD que trabajan a tiempo parcial o que están compartidos entre varias organizaciones pueden enfrentarse a un conflicto permanente en la asignación de tiempo y esfuerzos, debilitando su independencia e imparcialidad como resultado de su posición y, por tanto, dando lugar a posibles conflictos de intereses a la hora de priorizar a qué responsable asesorar o supervisar, o los términos de dicha supervisión y asesoramiento.

Un único DPD que presta servicio de asesoramiento y supervisión a un número de responsables superior al que razonablemente pueda atender con la debida dedicación y accesibilidad difícilmente podría demostrar que dicho asesoramiento se produce y, además, al realizar su asesoramiento y supervisión**,** entraría en un claro conflicto de intereses a la hora de priorizar a un responsable por delante de otros.

6. Falta de independencia en la gestión

Cuando el DPD no tiene posibilidad de reportar al más alto nivel de dirección, puede ocurrir que, de un lado, su independencia se vea comprometida y, de otro lado, que la alta dirección no sea plenamente consciente de los riesgos de protección de datos que asume. Esta situación se produce cuando entre el DPD y la alta dirección existen intermediarios que trasladan al responsable el asesoramiento y la supervisión del DPD.

Del mismo modo, cuando el DPD recibe instrucciones del responsable o del encargado, se encuentra en una situación en la que la falta de independencia puede derivar en un conflicto de intereses en el desarrollo de su labor de asesoramiento y supervisión, ya que las actuaciones de supervisión estarán orientadas a valorar positivamente las órdenes del responsable y no a garantizar los derechos, libertades e intereses de las personas físicas.

7. Falta de salvaguardas internas

La ausencia de procedimientos internos y la falta de aprobación de políticas de protección de datos que garanticen la independencia del DPD y eviten la existencia de conflictos de intereses en su designación y, tras esta, en el desempeño de sus funciones ponen de manifiesto un problema de gobernanza de la organización.

Es recomendable que las organizaciones determinen los puestos incompatibles, elaboren normas internas para evitar situaciones de conflicto, incluyan una explicación general y clara sobre los mismos, verifiquen y declaren que su DPD no tiene conflicto de intereses en el momento de su nombramiento y establezcan salvaguardas en las normas internas y contratos de servicios que eviten el riesgo de que concurra cualquier tipo de conflicto o incompatibilidad.

No obstante, y como se señala en la ISO 37009:2025, el conflicto de intereses puede aparecer en el desarrollo de las actividades de una organización en cualquier momento. En este sentido, las actividades del DPD no se encuentran exentas de posibles conflictos

de intereses. Gestionar los conflictos de intereses no es un formalismo, es la condición que permite al DPD asesorar con criterio y supervisar con objetividad, condiciones necesarias para que el responsable y el encargado del tratamiento puedan demostrar cumplimiento.

VIII. VÍAS DE AMPARO DEL DPD

En aquellos casos en que el DPD reciba presiones o injerencias, o en que se incumplan de cualquier modo las garantías de su estatuto, deberá disponer de vías para solicitar amparo.

El artículo 38.3 del RGPD prohíbe expresamente que el DPD sea destituido o sancionado por el desempeño de sus funciones. El artículo 36.2 de la LOPDGDD concreta una protección mayor para el DPD persona física integrada en la organización del responsable o encargado, según la cual el DPD interno solo podrá ser removido o sancionado si incurre en dolo o negligencia grave en el ejercicio de sus funciones.

Además, tal y como se ha comentado en el apartado V, la jurisprudencia del TJUE ha interpretado ampliamente la noción de medida desfavorable y a la luz de esta doctrina las autoridades de control, teniendo en cuenta el considerando 97 del RGPD, vienen a plantear la necesidad de que los DPD estén en condiciones de desempeñar sus funciones y cometidos de manera independiente, considerando que el marco de protección del DPD se orienta a evitar cualquier medida desfavorable o represalia que condicione su independencia en el ejercicio de sus funciones como, por ejemplo, la retirada sustancial de funciones, la supresión de los recursos indispensables, el aislamiento jerárquico o el bloqueo en la promoción profesional. Vías internas

1. Reporte directo al más alto nivel jerárquico

Ante cualquier obstrucción o injerencia, el DPD deberá poder ejercitar su facultad y garantía de acudir directamente a la alta dirección (consejo de administración, dirección general o subsecretaría) sin pasar por intermediarios ni filtros.

2. Canal del informante y canal ético

El DPD contará con acceso al sistema interno de información a través del canal del informante (Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción) de la propia organización para reportar formalmente presiones, represalias o conflictos de intereses que menoscaben o puedan menoscabar su independencia.

3. Documentación y trazabilidad del desamparo o discrepancia

De conformidad con el artículo 36.4 de la LOPDGDD, cuando el DPD detecte una vulneración relevante o una falta grave de recursos y/o garantías, deberá documentarla formalmente y comunicarla de inmediato a los órganos de administración.

A. CONSULTA O DENUNCIA ANTE LA AUTORIDAD DE CONTROL

1. Consulta a la autoridad de control

El DPD podrá realizar consultas e informar sobre dudas o situaciones que afecten al cumplimiento de sus funciones y del RGPD. Estará siempre amparado por el deber de secreto y confidencialidad que vincula a las actuaciones de la autoridad de control.

2. Inicio de procedimiento de investigación o sancionador

El incumplimiento, por parte del responsable o encargado, de las obligaciones relativas a la posición, recursos e independencia del DPD (artículos 37 a 39 del RGPD) constituye una infracción legal.

La autoridad de control podrá acordar actuaciones previas de investigación o acordar el inicio de un procedimiento sancionador para aplicar las medidas correctoras o multas administrativas que en su caso correspondan.

B. VÍA JUDICIAL

Jurisdicción social o contencioso-administrativa

En caso de despido, remoción del puesto, sanción o modificación sustancial de condiciones adoptados como represalia por el ejercicio independiente de sus funciones, el DPD podrá acudir a los tribunales para solicitar la invalidez de la medida y la restitución de sus condiciones e independencia.

En el caso de relación laboral**,** podrá acudir a la jurisdicción social y**,** en el caso de empleados públicos**,** al orden contencioso-administrativo o al orden social según proceda.

IX. CONCLUSIÓN

La efectividad de la figura del DPD exige que su designación, su integración en la organización y las condiciones de ejercicio de sus funciones respondan a un mismo objetivo: garantizar un asesoramiento especializado y una supervisión independiente que contribuyan al cumplimiento de la normativa de protección de datos y permitan demostrarlo. Estas garantías deben mantenerse durante todo el desempeño de sus funciones y proyectarse también sobre las decisiones que afecten a su permanencia o cese.

La designación del DPD no debe reducirse a un trámite formal. Resulta recomendable documentar expresamente su nombramiento, sus funciones, su posición organizativa, los recursos asignados y los canales mediante los que accederá al más alto nivel de dirección. Esta definición facilita su integración efectiva en la gobernanza de la organización y previene discrepancias posteriores sobre el alcance de sus competencias y las condiciones de su actuación. La designación de un órgano colegiado permite

adaptar la figura del DPD a las características de una organización y supone una garantía de continuidad de la figura del DPD y, en definitiva, una garantía de los recursos asignados a las funciones del DPD.

La falta de recursos económicos afecta directamente a la independencia del DPD pues, de un lado, puede condicionarse su asesoramiento y supervisión con la consecución de determinados objetivos económicos de la entidad en la que presta servicio y, de otra parte, puede imposibilitar el ejercicio de sus funciones. Este segundo caso se produce cuando se pretende prestar un servicio de DPD a un desmesurado número de responsables y encargados o cuando, simplemente, el coste de un servicio de DPD contratado es irrisorio o temerariamente insuficiente para proporcionar un servicio de DPD efectivo, situación particularmente crítica cuando se trata de responsables de las administraciones públicas.

Para que el DPD pueda asesorar con criterio y supervisar con objetividad, debe gozar de un estatus que le permita actuar libremente. El responsable o el encargado del tratamiento deben garantizar su participación adecuada y en tiempo oportuno en las cuestiones relativas a la protección de datos, el acceso a la información necesaria y la disponibilidad de recursos materiales y humanos, tiempo, formación continua y apoyo organizativo suficientes. Asimismo, el DPD no debe recibir instrucciones sobre el contenido de su asesoramiento, sus investigaciones o sus actuaciones de supervisión.

El reporte directo al más alto nivel jerárquico constituye una garantía material de independencia. La organización debe disponer de cauces efectivos para que el DPD comunique sus recomendaciones, eleve riesgos y vulneraciones relevantes y exponga las necesidades que afecten al desempeño de sus funciones. Esta interlocución debe permitir que la dirección conozca y considere su asesoramiento antes de adoptar decisiones y que las cuestiones que requieran una actuación inmediata se comuniquen oportunamente.

Los mecanismos de reporte y rendición de cuentas deben ser proporcionados a la naturaleza, dimensión, complejidad y riesgo de los tratamientos. El RGPD no impone un modelo uniforme de informe ni una obligación general de elaborar una memoria anual. Los informes periódicos constituyen una buena práctica, especialmente útil en organizaciones complejas, que puede complementarse con actas, comunicaciones documentadas, registros de recomendaciones o informes específicos. Lo relevante es acreditar la intervención efectiva del DPD y la adecuada consideración de su criterio.

La documentación del asesoramiento y de las actuaciones de supervisión facilita la trazabilidad de las decisiones. Cuando la organización se aparte de las recomendaciones del DPD, resulta recomendable dejar constancia de las razones que justifican esa decisión. Esta práctica refuerza la responsabilidad proactiva sin alterar el carácter no vinculante de sus recomendaciones ni trasladarle la responsabilidad de decidir sobre los tratamientos.

En ningún caso el DPD puede ocupar un cargo en la organización que le lleve a determinar los fines y los medios del tratamiento de datos personales. Esta limitación no impide que, en el ejercicio de sus funciones de asesoramiento y supervisión, el DPD participe en el análisis de dichos fines y medios y formule recomendaciones sobre su adecuación al RGPD o proponga alternativas que permitan alcanzar los fines legítimos perseguidos por el responsable con un menor impacto sobre los derechos y libertades de las personas. La decisión final corresponderá, en todo caso, al responsable del tratamiento.

Los puestos y situaciones susceptibles de generar conflictos de intereses no constituyen una lista cerrada. Las organizaciones deben evaluarlos atendiendo a su actividad, estructura, distribución de competencias y relaciones de las personas implicadas**,** teniendo en cuenta los fines, el contexto, el alcance y la naturaleza de sus tratamientos. Esta evaluación debe realizarse antes del nombramiento y mantenerse de forma continua, puesto que los conflictos pueden aparecer durante el ejercicio de las funciones. La acumulación de cometidos, la prestación externa de servicios y las relaciones con responsables o encargados deben examinarse considerando si comprometen la objetividad del DPD o le llevan a supervisar sus propias decisiones o actividades.

Contar con una política de gestión de conflictos de intereses en la organización que incluya salvaguardas claras y documentación consistente es esencial. Resulta recomendable identificar los puestos incompatibles, establecer procedimientos para comunicar y evaluar situaciones sobrevenidas, definir los mecanismos de abstención y recusación e incorporar salvaguardas en las normas internas y en las condiciones de contratación. Estas medidas deben ser conocidas por la organización y revisarse para comprobar su efectividad.

La protección de la independencia del DPD comprende tanto la prohibición de destituirlo o sancionarlo por desempeñar sus funciones como la protección frente a represalias vinculadas a su asesoramiento o supervisión. Esta garantía no equivale a una inamovilidad absoluta. Cuando el DPD sea una persona física integrada en la organización, deberá tenerse en cuenta la protección reforzada prevista en el artículo 36.2 de la LOPDGDD.

Las decisiones sobre su permanencia, funciones, recursos o posición institucional deben examinarse por sus efectos materiales. Una reducción significativa de medios, la pérdida de acceso directo a la dirección o la retirada de competencias esenciales pueden comprometer su independencia aun cuando no exista un cese formal. Por ello, resulta recomendable recabar previamente su parecer, evaluar el impacto de estas medidas y documentar las razones que justifican su adopción.

La designación efectiva, la comunicación directa con la dirección, los recursos suficientes, la prevención de conflictos de intereses y las garantías frente a represalias deben articularse conjuntamente. Su finalidad es que el DPD pueda asesorar con criterio,

supervisar con objetividad y contribuir a una cultura organizativa de protección de datos. El respaldo institucional a sus funciones facilita el cumplimiento y la rendición de cuentas, preservando la responsabilidad que corresponde al responsable y al encargado del tratamiento y protegiendo los derechos, las libertades y los intereses de las personas físicas.

En definitiva, este documento no pretende establecer un modelo organizativo único, ni crear nuevas obligaciones jurídicas, sino facilitar la interpretación y aplicación práctica de las garantías previstas en el ordenamiento, reforzar la independencia funcional del DPD y promover su adecuada integración en la gobernanza de las organizaciones, sin sustituir la evaluación jurídica y organizativa que corresponda realizar en cada caso.

X. REFERENCIAS

A. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

- AEPD - Plan Estratégico 2025-2030, presentado el 3 de julio de 2025
- AEPD - Plan de actuación 2026
- AEPD - Recomendaciones para fortalecer el cumplimiento de la normativa de protección de datos en la Administración General del Estado, 14 de julio de 2026
- AEPD - La AEPD impulsa un modelo común de cumplimiento en el sector público con recomendaciones y próximas acciones (nota de prensa, 14 de julio de 2026)
- AEPD - Resultados de la acción europea que ha analizado la designación y situación de los delegados de protección de datos (nota de prensa, 2024)
- AEPD - Instrucción 1/2021, de 2 de noviembre, por la que se establecen directrices respecto de la función consultiva de la Agencia (BOE de 5 de noviembre de 2021)
- AEPD - Informe jurídico 0170/2018, de 12 de noviembre de 2018, sobre la compatibilidad entre el delegado de protección de datos y el responsable de seguridad del Esquema Nacional de Seguridad
- AEPD - Informe jurídico 0167/2018, sobre la separación entre el delegado de protección de datos y el responsable de seguridad del Esquema Nacional de Seguridad
- AEPD - Informe jurídico 0037/2020, sobre la designación de un mismo delegado de protección de datos para varios responsables o encargados y los requisitos de su nombramiento
- AEPD - Informe jurídico 0048/2021, sobre una política de seguridad de la información y la posición del delegado de protección de datos en la estructura de seguridad
- AEPD - Informe jurídico 0038/2023 (ref. 0096/2022), sobre la posición jurídica y las funciones del delegado de protección de datos
- AEPD - Informe jurídico 0034/2023
- AEPD - Resolución del procedimiento sancionador PS/00345/2022 (EXP202201681), de 19 de julio de 2023, sobre la designación como delegado de protección de datos del secretario de un colegio profesional, confirmada por la Sentencia de la Audiencia Nacional 139/2026
- AEPD - Resolución de 14 de junio de 2024 del recurso de reposición interpuesto contra la resolución del procedimiento sancionador PS/00382/2023

(EXP202211394), sobre el conflicto de intereses del delegado de protección de datos que presenta alegaciones en nombre del responsable

- AEPD - Resolución del procedimiento sancionador PS/00548/2024 (EXP202316729), de 5 de marzo de 2026, sobre la incompatibilidad entre las funciones de delegado de protección de datos y de responsable del sistema interno de información
- AEPD - Esquema de certificación de delegados de protección de datos (Esquema AEPD-DPD), versión 1.4, de 23 de diciembre de 2019
- AEPD - Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, junio de 2021
- AEPD - Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo
- AEPD - Protección de datos desde el diseño en los contratos de la Administración Pública (blog)
- Korff, D. y Georges, M. (proyecto T4DATA) - El manual del DPD (2019), edición española publicada por la AEPD

B. Comité Europeo de Protección de Datos y Supervisor Europeo de Protección de Datos

- GT29/CEPD - Directrices sobre los delegados de protección de datos (WP243 rev.01), adoptadas el 13 de diciembre de 2016 y revisadas el 5 de abril de 2017, asumidas por el CEPD el 25 de mayo de 2018
- CEPD - 2023 Coordinated Enforcement Action – Designation and Position of Data Protection Officers. Informe adoptado el 16 de enero de 2024
- CEPD - Directrices 9/2022 sobre la notificación de violaciones de la seguridad de los datos personales en virtud del RGPD, versión 2.0, adoptadas el 28 de marzo de 2023
- SEPD - Supervisory Guidance – Role of the Data Protection Officers in EU institutions, bodies, offices and agencies, adoptada el 18 de diciembre de 2025 (versión 1.1, de 5 de febrero de 2026)
- SEPD - Decisión 01/2026 del Supervisor Europeo de Protección de Datos, de 16 de enero de 2026, sobre las normas de aplicación del requisito de consentimiento previo del SEPD para la destitución de los delegados de protección de datos (DOUE L 2026/199, de 29 de enero de 2026)
- SEPD - Position Paper on the role of Data Protection Officers of the EU institutions and bodies, 30 de septiembre de 2018

C. AUTORIDADES AUTONÓMICAS

- CTPDA - Modelo de instrucción interna para fortalecer el papel del Delegado de Protección de Datos en las entidades del sector público andaluz, febrero de 2025
- CTPDA - Resolución de 16 de junio de 2026, por la que se aprueba el Plan de Control e Inspección sobre Protección de Datos en el Sector Público Andaluz 2026-2027 (BOJA n.º 118, de 22 de junio de 2026)
- APDCAT - Dictamen CNS 17/2024, sobre las funciones del delegado de protección de datos
- APDCAT - Dictamen CNS 29/2022

D. AUTORIDADES DE CONTROL DE OTROS ESTADOS

- CNIL - Le rapport d'activité du DPO : piloter la conformité et valoriser ses actions (guía y modelo de informe de actividad, 27 de abril de 2026)
- CNIL - Guide pratique RGPD – Délégués à la protection des données (2022), con modelo de carta de misión
- CNIL - Délégué à la protection des données: identifier et gérer les conflits d'intérêts liés à la fonction de DPO (10 de agosto de 2026)
- Autorité de protection des données (Bélgica) - Permettre au délégué à la protection des données d'exercer ses missions en toute indépendance (actualizado el 24 de enero de 2024)
- Autorité de protection des données (Bélgica) - Décision quant au fond n° 18/2020 du 28 avril 2020 (conflicto de intereses del delegado de protección de datos)
- Autorité de protection des données (Bélgica) - Recommandation n° 04/2017 du 24 mai 2017 relative à la désignation d'un délégué à la protection des données et l'admissibilité du cumul avec d'autres fonctions
- Garante per la protezione dei dati personali (Italia) - Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico (Provvedimento del 29 aprile 2021, n. 186; Gazzetta Ufficiale n. 132, de 4 de junio de 2021)
- Autoriteit Persoonsgegevens (Países Bajos) - Positionering van de FG. Uitgangspunten: rollen, processen en verantwoordelijkheden (junio de 2021)
- Data Protection Commission (Irlanda) - Guidance on appropriate qualifications for Data Protection Officers

- Data Protection Commission (Irlanda) - Decision IN-18-12-01, Department of Employment Affairs and Social Protection, 10 de mayo de 2021 (participación adecuada del DPD y ausencia de instrucciones)
- Oficina del Defensor de la Protección de Datos (Finlandia) - Designating a data protection officer
- Datatilsynet (Dinamarca) - Vejledning om databeskyttelsesrådgivere (diciembre de 2017)
- Integritetsskyddsmyndigheten (Suecia) - IMY klar med fördjupade granskningar av dataskyddsombudens roll (2024; decisiones de supervisión sobre el papel y la posición de los delegados de protección de datos en el marco de la acción coordinada europea)
- Commission nationale pour la protection des données (Luxemburgo) - Délibération n° 18FR/2021 du 31 mai 2021 y demás decisiones de la campaña de auditorías temáticas sobre la función del delegado de protección de datos (2021)
- Datatilsynet (Noruega) - Sanctions imposed on Telenor ASA for lack in the organisation of the data protection officer and lack of internal control (decisión de 10 de marzo de 2025)

E. ASOCIACIONES PROFESIONALES, ESTÁNDARES Y OTROS

- ISO - ISO 37009:2025, Conflict of interest in organizations — Guidance
- BvD – Berufsverband der Datenschutzbeauftragten Deutschlands - Positionspapier Aufwandsabschätzungen DSB (abril de 2020)
- ISMS Forum – Data Privacy Institute - El Libro Blanco del DPO, II edición (febrero de 2025)
- CEDPO – Confederation of European Data Protection Organisations - Minimum qualifications for Data Protection Officers (30 de mayo de 2016)
- CEDPO – Confederation of European Data Protection Organisations - Follow-up letter on the WP29 Guidelines on Data Protection Officers (15 de febrero de 2017)
- ENISA - Mapping NIS2 obligations with ECSF role profiles (junio de 2025)
- IAPP - The most iconic DPA decisions on DPOs and what you should take from them (2023)
- AEC – Club del DPD - Conflictos de interés del DPD (I Insight exclusivo Club DPD, 2023; material divulgativo)

F. JURISPRUDENCIA

- TJUE, sentencia de 22 de junio de 2022, Leistritz, C-534/20, ECLI:EU:C:2022:495.
- TJUE, sentencia de 9 de febrero de 2023, X-FAB Dresden, C-453/21, ECLI:EU:C:2023:79.
- TJUE, sentencia de 9 de febrero de 2023, KISA, C-560/21, ECLI:EU:C:2023:81.
- Tribunal Supremo (Sala de lo Social), sentencia de 22 de septiembre de 2026, rec. 384/2025.
- Audiencia Nacional (Sala de lo Contencioso-Administrativo, Secc. 1.ª), sentencia 139/2026, de 18 de marzo, rec. 894/2023.
- Tribunal Superior de Justicia de Madrid (Sala de lo Social), sentencia de 2026 Sentencia STSJ M 7356/2026 - ECLI:ES:TSJM:2026:7356 y sentencia 910/2021, de 29 de diciembre, rec. 476/2021 [V].