II EDICIÓN
EL LIBRO BLANCO DEL DPO

isms forum dpi DATA PRIVACY INSTITUTE

FEBRERO 2025

AUTORES

COORDINACIÓN	Carlos A. Saiz
REVISIÓN	Javier Lomas
PARTICIPANTES	Alberto Casaseca
	Alberto Ribes
	Araceli Fernández
	Aranzazu Herráez
	Esmeralda Saracibar
	Esther García
	Josep Bardallo
	María Jesús Casado
	Marta Cañas
	Óscar Antonio Sánchez
	Patricia Mendoza
	Pilar Pascual
	Rubén Cabezas
	Sonia Beulax
GESTIÓN DEL PROYECTO	Beatriz García
DISEÑO/MAQUETACIÓN	Lydia García

CONTENIDOS

CONTENIDO

1 INTRODUCCIÓN Y CONTEXTO ACTUAL

1.1. Evolución y aprendizajes: razones para una segunda edición

Han pasado más de cinco años desde la publicación de la primera edición del ***Libro Blanco del DPO***[1], un periodo en el que la figura del Delegado de Protección de Datos (en adelante el DPO), ha evolucionado y consolidado su papel en las organizaciones. Lo que en un principio se percibía como un nuevo requisito normativo ha adquirido una dimensión estratégica, convirtiéndose en una pieza clave en la gestión de la privacidad y el cumplimiento normativo.

El contexto no ha cambiado solo desde el punto de vista normativo o judicial. La transformación digital, el crecimiento exponencial de los volúmenes de datos y la irrupción de la inteligencia artificial han redefinido los retos a los que se enfrenta el DPO. En este sentido, la madurez de los programas de privacidad y la creciente necesidad de integrar la protección de datos en el modelo de gobernanza corporativa también han cobrado protagonismo.

En estos años hemos ido aprendido mucho sobre los distintos modelos organizativos del DPO. Desde su ubicación en estructuras internas hasta su externalización o la configuración de equipos colegiados, cada organización ha encontrado su propio camino para garantizar la eficacia e independencia de esta función.

Además, las resoluciones de las autoridades de protección de datos y de los tribunales, tanto nacionales como europeos, han comenzado a pronunciarse sobre aspectos clave que afectan a esta figura, aportando interpretaciones que están redefiniendo su rol en la privacidad y protección de datos. Estas decisiones, aunque todavía escasas, están empezando a definir con mayor precisión los límites y obligaciones del DPO, ofreciendo pautas sobre su independencia, los conflictos de intereses, la dotación de recursos adecuados, la diligencia exigible en el cumplimiento de sus funciones y los riesgos asociados a una gestión deficiente de la protección de datos.

[1] *Libro Blanco del DPO – isms forum spain & data privacy institute*

Uno de los hitos más relevantes en esta evolución ha sido ***Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos***[2] (en adelante, Esquema AEPD-DPD), para que las personas responsables puedan seleccionar a los y las profesionales cuyas competencias como DPO hayan sido certificadas por entidades acreditadas por la Entidad Nacional de Acreditación (en adelante, ENAC), reforzando su profesionalización y reconocimiento dentro de las organizaciones. Este paso ha permitido establecer estándares más claros sobre sus competencias y responsabilidades, proporcionando a las empresas un criterio objetivo para evaluar la idoneidad de sus DPO y garantizando un mayor nivel de cualificación en el desempeño de sus funciones.

Más recientemente, la entrada en vigor de la normativa de la Unión Europea sobre Inteligencia Artificial (RIA) ha introducido nuevos retos en la gestión del tratamiento de datos personales. La regulación establece criterios específicos para garantizar la privacidad en el uso de la IA, exigiendo una mayor supervisión y medidas adicionales de cumplimiento, lo que refuerza aún más el papel del DPO en este ámbito.

En respuesta a estos avances, esta segunda edición del Libro Blanco del DPO no es simplemente una actualización de referencias normativas o un repaso de lo que ya conocíamos. Es una guía reflexiva y práctica sobre lo que hemos empezado a aprender en estos cinco años, los nuevos desafíos que han surgido y las mejores prácticas que pueden ayudar a los DPO a afrontar su labor con éxito. Y esto es solo el principio.

En esta nueva edición, no solo recogemos el marco normativo y los principios fundamentales de su función, sino que también incorporamos experiencias prácticas que han marcado la madurez del modelo de gobierno de la privacidad en las organizaciones, tanto en el sector público como en el privado, consolidándose como una pieza clave en el ecosistema de la protección de datos. Esta edición del Libro Blanco pasa del plano teórico a la realidad organizativa, donde el DPO interactúa con distintas líneas de defensa y donde su encuadre sigue siendo objeto de análisis y evolución.

Con este enfoque práctico que ha guiado la elaboración de esta guía, hemos integrado herramientas y metodologías que permiten optimizar la gestión del DPO. Destaca la inclusión de un apartado dedicado a las metodologías de reporte, donde se aborda la importancia de los indicadores clave de rendimiento (KPIs) como una estrategia eficaz para evaluar el grado de cumplimiento, supervisar la función y proporcionar a la alta dirección información clave para la toma de decisiones informadas. La consolidación de modelos organizativos, la definición de funciones y la interacción del DPO con otras áreas estratégicas de la organización son algunos de los aspectos que hemos analizado a partir de la experiencia de múltiples entidades.

Asimismo, en esta edición hemos profundizado en los mecanismos de independencia del DPO, no como un fin en sí mismo, sino como un medio indispensable para garantizar que pueda desempeñar sus funciones de manera efectiva y sin interferencias. Este análisis se ve reforzado con decisiones recientes de autoridades de protección de datos y jurisprudencia europea que han clarificado la importancia de preservar esta independencia, ofreciendo ejemplos concretos de cómo puede verse comprometida y las consecuencias de ello.

El papel del DPO ya no es una incógnita como lo era hace cinco años. La experiencia acumulada ha contribuido a perfilar con mayor claridad su función y responsabilidades. Sin embargo, el futuro presenta nuevos retos. La irrupción de la inteligencia artificial y su impacto en la protección de datos personales han abierto un nuevo escenario en el que la figura del DPO será clave para garantizar un desarrollo responsable y alineado con los principios

[2] *Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos*

de privacidad y gobernanza. La gestión de los riesgos asociados a la IA y la evolución de su regulación están configurando un campo en el que la función del DPO tendrá un protagonismo creciente.

Con esta actualización, el Libro Blanco busca proporcionar un marco más completo y adaptado a la realidad actual del DPO, subraya la evolución del DPO en estos años, y destaca la importancia de los KPIs, los modelos organizativos, la independencia y el impacto de la IA, facilitando por tanto su labor en un entorno donde la privacidad, la seguridad de los datos y el cumplimiento normativo continúan evolucionando a un ritmo acelerado.

Esperamos que esta obra sea una herramienta útil para todos aquellos que desempeñan esta función, así como para quienes trabajan en estrecha colaboración con ellos.

> ***"La privacidad sigue evolucionando y, con ella, la figura del DPO. Es momento de seguir aprendiendo y adaptándonos a un entorno en constante cambio."***

1.2. Marco normativo

La derogada Directiva 95/46/CE hizo referencia a la figura del DPO bajo la denominación de encargado de los datos personales, en relación con la excepción a la obligación de notificación de los ficheros a la autoridad de control. Esta directiva permitió que los Estados Miembros incorporaran esta figura en su normativa nacional, aunque en España no se adoptó, optándose en su lugar por la figura obligatoria del Responsable de Seguridad, con atribuciones y un enfoque de actuación diferente.

Realmente, la primera e inevitable referencia legislativa relativa al DPO corresponde al **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 (en adelante "RGPD") que regula esta figura en la **sección 4 del Capítulo IV**, artículos 37, 38, 38, sin olvidar el **Considerando 97.** Si bien el RGPD no inventó el concepto de Delegado de Protección de Datos, sí impuso nuevos requisitos a escala de la UE, estableciendo las condiciones para su nombramiento, sus facultades y su posición dentro de las estructuras organizativas.

En el ámbito nacional, los **artículos 34 al 37 de la Ley Orgánica 3/2018, de 5 de diciembre**, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, **LOPDGDD**) amplían y perfilan lo establecido en el RGPD respecto a esta figura, concretando aspectos como los supuestos de designación obligatoria y su relación con la Administración Pública.

La evolución del marco normativo ha estado acompañada por documentos clave, como las **Directrices WP243** del Grupo de Trabajo del Artículo 29 (en adelante, **GT29**), que fueron posteriormente refrendadas por su sucesor, el **European Data Protection Board (en adelante, EDPB)**, en su primera reunión plenaria tras su creación.

Antes de la entrada en vigor del RGPD, el GT29 destacó el papel de los entonces denominados Responsables de Protección de Datos (en adelante, **RPD**) como «una piedra angular de la rendición de cuentas». Sus **Directrices sobre los RPD de 2017** fueron posteriormente adoptadas por el EDPB tras la entrada en vigor del RGPD, afirmando que estos profesionales serían *«el núcleo del nuevo marco jurídico para muchas organizaciones».*

Asimismo, resulta fundamental tener en cuenta las guías, respuestas, opiniones e informes de la AEPD, en particular el **informe 164/2018,** que analiza la incompatibilidad entre el DPO y el Responsable de Seguridad. También cabe destacar la **acción coordinada aprobada** por el EDPB en enero de 2023, centrada en la designación y posición de los Delegados de Protección de Datos.

Todo ello constituye una referencia esencial que será analizada a lo largo del presente Libro Blanco. Si bien el RGPD y la LOPDGDD establecen el núcleo del marco normativo del DPO, su ámbito de actuación no se limita a estas normas. En su labor diaria, también deben considerarse otras regulaciones, entre ellas:

- La **Ley de Servicios de la Sociedad de la Información y Comercio Electrónico** (en adelante, LSSI).
- La **Ley General de Telecomunicaciones** (en adelante, LGT), que transpone la **Directiva 2002/58/CE** (e-Privacy), actualmente en proceso de revisión para su conversión en reglamento comunitario.
- La **Directiva (UE) 2016/1148** del Parlamento Europeo y del Consejo (Directiva NIS), relativa a la seguridad de redes y sistemas de información, que impacta en sectores donde la protección de datos se vincula con la ciberseguridad.

Además, es imprescindible tener en cuenta los **dictámenes, opiniones y guías del GT29 y el EDPB**, así como las resoluciones y criterios interpretativos de la **AEPD y de las autoridades autonómicas de protección de datos.** También se debe prestar atención a los pronunciamientos de **órganos jurisdiccionales**, dado el creciente desarrollo jurisprudencial en materia de protección de datos.

Por último, no podemos obviar el impacto de los **estándares y normativas internacionales** en la función del DPO. En este sentido, la labor de la Organización Internacional de Normalización (ISO) es clave. La **ISO/IEC 27701:2021** proporciona directrices sobre la gestión de la privacidad y la protección de la información personal, permitiendo a las organizaciones demostrar su cumplimiento normativo a nivel global.

En el ámbito de la seguridad de la información, es relevante considerar los estudios y recomendaciones de organismos especializados, como:

- La **Agencia Europea de Seguridad de las Redes y de la Información (ENISA).**
- El **CCN-CERT (Centro Criptológico Nacional).**
- El **INCIBE (Instituto Nacional de Ciberseguridad).**

Todos estos elementos conforman un ecosistema normativo dinámico y en constante evolución, que define el marco de actuación del DPO y su papel dentro de las organizaciones.

2 LA FUNCIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS

En la actualidad, no parece que exista duda alguna respecto a que el rol y la función del delegado de protección de datos es crucial para el cumplimiento de la normativa en materia de protección de datos. Ya antes de la entrada en vigor del RGPD, el Grupo de Trabajo del Artículo 29 calificaba a los delegados de protección de datos como "una piedra angular de la rendición de cuentas"; y el actual Comité Europeo de Protección de Datos, tras la entrada en vigor del RGPD, indicó que los delegados de protección de datos serían "el corazón de este nuevo marco legal", llegando a afirmar recientemente que nos encontramos en un momento en el que, a la vista de la entrada en vigor de numeras normas en relación con el mercado digital (ley del mercado digital, la ley de datos, la ley de servicios digitales, el reglamento de inteligencia artificial, etc.) "el papel de los delegados de protección de datos parece estar cambiando", ya que se observa que cada vez más que "se están asignando a los delegados de protección de datos nuevas funciones relacionadas con la inteligencia artificial, la ética, la gobernanza de datos, y los espacios de datos".

2.1. Designación del delegado de protección de datos

El considerando 97 RGPD señala: *"Al supervisar la observancia interna del presente Reglamento,* ***el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos*** *si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas* ***actividades principales*** *consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con* ***sus actividades primarias y no están relacionadas con el tratamiento de datos personales***

como actividades auxiliares. *El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente".*

Resulta sumamente interesante este Considerando porque en él se establen los criterios generales, que luego desarrolla el propio RGPD en su articulado, y que permiten a las organizaciones saber cuándo va a ser necesario u obligatorio la designación o el nombramiento de un Delegado de Protección de Datos.

En este sentido, las primeras conclusiones que podemos obtener es que resulta obligatorio el nombramiento de un DPO cuando:

- El tratamiento de datos lo lleva a cabo una autoridad pública
- Cuando las actividades principales de la organización (responsable o encargado del tratamiento) consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados
- Cuando las actividades principales de la organización (responsable o encargado del tratamiento) consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales

Por su parte, el artículo 37.1 RGPD establece tres criterios para los que se considera obligatorio el nombramiento de un delegado de protección de datos:

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

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

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

Las Directrices del GT29 introdujo algunas aclaraciones sobre diferentes aspectos o conceptos de estos criterios[3][4]. A saber:

- El concepto de "actividad principal" debe interpretarse de forma incluyente de todas aquellas actividades que, sin ser coincidentes con el objeto social, son indisociables del mismo, excluyendo aquellas actividades soporte que aun siendo necesarias para el cumplimiento de la actividad principal no son indisociables de la misma.

- "Gran escala" no puede cuantificarse de forma general sino debe realizarse teniendo en cuenta el número de interesados afectados, su proporción frente a la población correspondiente, el volumen y variedad de los datos, la duración o permanencia del tratamiento o el alcance geográfico del mismo .

- "Observación habitual y sistemática". El concepto "habitual" debe interpretarse con alguno de los siguientes significados: continuado o que se produce a intervalos concretos durante un período concreto recurrente o repetido en momentos prefijados que tiene lugar de manera constante o periódica. Por lo que se refiere a *"sistemática"* debe interpretarse como aquello que se produce de acuerdo con un sistema o que está ejecutado de forma preestablecida, organizada o metódica .

[3] *Esquema certificación aepd (punto 7.2. y 7.1.);*

[4] *Informe Jurídico 2023-0038;*

Sin perjuicio de lo establecido en el RGPD, la LOPDGDD en su artículo 34.1 realiza una enumeración detallada de entidades que están obligadas a designar un DPO. Sin otra pretensión que facilitar el acceso a la misma, procedemos aquí a su enumeración:

a) Los colegios profesionales y sus consejos generales

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que 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.

Si algo escapa a la enumeración anterior, el GT29 recomienda que los responsables y encargados del tratamiento documenten el análisis interno realizado para determinar si debe nombrarse o no un DPO. En todo caso, la LOPDGDD, en su art. 34.2 se refiere a la posible designación voluntaria del DPO que en muchos casos puede ser recomendable, al menos por las siguientes razones:

- La graduación de la sanción atendiendo a la existencia de un DPO en la organización cuando no fuere obligatorio (artículo 76.h LOPDGDD).

- La Intervención del DPO en la resolución de reclamaciones, tanto aquellas que le dirijan los ciudadanos, cuando opten por esta vía antes de plantear una reclamación ante la AEPD, como las reclamaciones que la AEPD decida trasladarle con carácter previo al inicio de un expediente sancionador. De esta forma, con carácter general, si el DPO consigue que se resuelva la reclamación, y sin perjuicio de que el interesado posteriormente se dirija a la AEPD, no se iniciaría expediente sancionador (artículo 37 LOPDGDD).

- El mayor aseguramiento para la organización en relación con el cumplimiento en privacidad, derivado de la existencia de una posición en la organización dedicada específicamente y de forma regulada a esta actividad.

Recientemente, el propio Comité Europeo de Protección de Datos , ha señalado que tanto el responsable como el encargado del tratamiento pueden optar por designar un DPO de forma voluntaria; siendo extremadamente útil el contar con un experto en protección de datos, que en los procesos de planificación y toma de decisiones de cualquier empresa, ayude con el cumplimiento de la normativa de protección de datos y especialmente con los principios de la rendición de cuentas, la protección de datos desde el diseño y por defecto y con la obligación de implementar medidas técnicas y organizativas adecuadas para el cumplimiento del RGPD, entre muchas otras.

Por otra parte, el DPO será designado, ex. Artículo 37.5 RGPD, atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39 RGPD; pudiendo tener carácter interno o externo (art. 37. 6 RGPD). **El artículo 37, apartado 2, del RGPD permite a un grupo empresarial designar un único delegado de protección de datos (DPO), siempre que este "sea fácilmente accesible desde cada establecimiento".** En cuanto a la forma de realizar dicho nombramiento, designación y cese, según el art. 34.3 LOPDGDD, los responsables y encargados del tratamiento deberán comunicarlo 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, tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria; debiendo publicar sus datos de contacto y comunicarlos a la autoridad de control (art. 37.7 RGPD).

2.2. Funciones o tareas del delegado de protección de datos

Las funciones del DPO que el artículo 39 RGPD establece, como mínimo, son las siguientes:

a. **informar y asesorar** al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros

b. **supervisar** el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes

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

d. **cooperar** con la autoridad de control;

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

Recientemente, la Agencia Española de Protección de Datos ha tenido ocasión de pronunciarse, en el informe jurídico 0038/2023, sobre una serie de cuestiones sumamente interesantes en relación con las funciones del DPO, diferenciando entre funciones "decisoras" (que corresponden al responsable del tratamiento) y "asesoras o de supervisión" (que corresponden al DPO); aclarando lo siguiente[3][4]:

- Las funciones del DPO son únicamente de asesoramiento y supervisión, como indica el art. 39 RGPD, pero el DPO no tiene funciones de decisión, ya que estas corresponden al responsable o encargado del tratamiento, siendo el responsable quien decidirá sobre los fines y medios del tratamiento y sobre la forma en que finalmente serán tratados los datos personales .

[3] *Esquema certificación aepd (punto 7.2. y 7.1.);*

[4] *Informe Jurídico 2023-0038;*

- El listado de funciones del art. 39 RGPD es un listado de mínimos, pudiéndose asignar otras funciones al DPO, como por ejemplo la llevanza del registro de actividades de tratamiento; pero siempre respetando el carácter asesor y supervisor del DPO, sin que puedan implicar la intervención directa en la toma de decisiones referidas a los fines y medios del tratamiento, que afectaría a su independencia e implicarían la existencia de un conflicto de intereses .

- El DPO actúa como asesor y supervisor interno, por lo que ese puesto no puede ser ocupado por personas que, a la vez, tengan tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos (p.ej.: responsables de ITC, o responsables de seguridad de la información).

- El DPO asume principalmente funciones de asesoramiento y supervisión en beneficio del responsable o encargado. Sin embargo, como señala claramente el RGPD en diferentes preceptos, el responsable tendrá responsabilidad plena ante la ley por cualquier fallo en ese sentido, sin que, en ningún caso, dicha responsabilidad recaiga sobre el DPO.

- El DPO deberá facilitar al responsable o encargado toda la documentación derivada del ejercicio de sus funciones. El criterio no es vinculante para el responsable, aunque es recomendable que este deje documentadas las razones o motivos que le llevan a separase o no seguir el criterio del DPO.

- Separación de las funciones asesoras y supervisoras del DPO de las funciones de gestión o gobierno de la privacidad y protección de datos (que caen bajo la órbita del responsable o encargado del tratamiento) que podrían asignarse a un "responsable de privacidad y protección de datos" de manera separada a la función del DPO.

También la propia AEPD en el citado informe se refiere a las funciones de consulta previa a la autoridad de controle, señalando que: *"La función de consulta a la autoridad de control se encuadra, por consiguiente, entre las funciones propias del DPO, protegida por su independencia funcional, lo que implica que no puede recibir instrucciones respecto de su desempeño. De este modo, el responsable o encargado podrá solicitar el asesoramiento del DPO, y si éste lo estima oportuno, podrá formular consulta a la autoridad de control, pero sin que pueda recibir instrucciones al respecto".*

Finalmente, es importante recordar que el ejercicio de todas estas funciones de asesoramiento, supervisión y colaboración con la autoridad de control (tanto las asignadas normativamente como las que puedan ser asignadas voluntariamente por el responsable o encargado del tratamiento); el DPO, tal y como ha señalado la propia AEPD "está llamado a desempeñar un papel fundamental dentro del nuevo modelo de responsabilidad proactiva" debiendo actuar, según el art. 39.2 RGPD, con un claro enfoque a los riesgos que puedan derivarse de los tratamientos de datos personales, teniendo en cuenta la naturaleza, el alcance, el contexto y los propios fines del tratamiento .

2.3. Funciones del DPO, según Esquema de Certificación de la AEPD

Según el punto 7.2 del Esquema, las funciones genéricas del DPO se pueden concretar en tareas de asesoramiento y supervisión, entre otras, en las siguientes áreas:

1. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.

2. Identificación de las bases jurídicas de los tratamientos.

3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

4. Determinación de la existencia de normativa sectorial que pueda estipular condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.

5. Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.

6. Establecimiento de procedimientos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.

7. Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.

8. Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.

9. Identificación de los instrumentos para las transferencias internacionales de datos adecuados a las necesidades y características de la organización, y de las razones que justifiquen la transferencia.

10. Diseño e implantación de políticas de protección de datos.

11. Auditoría de protección de datos.

12. Establecimiento y gestión de los registros de actividades de tratamiento.

13. Análisis de riesgos de los tratamientos realizados.

14. Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.

15. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

16. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.

17. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.

18. Realización de evaluaciones de impacto sobre la protección de datos.

19. Relaciones con las autoridades de supervisión.

20. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

Para ello, según el punto 7.1. del esquema, el DPO deberá ser capaz de:

a) recabar la información necesaria para determinar las actividades de tratamiento;

b) analizar y comprobar la conformidad de las actividades de tratamiento con la normativa aplicable;

c) informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento;

d) recabar información para supervisar el registro de las operaciones de tratamiento;

e) asesorar en la aplicación del principio de la protección de datos por diseño y por defecto;

f) asesorar sobre:

- si se debe llevar a cabo o no una evaluación de impacto de la protección de datos y qué áreas o tratamientos deben someterse a auditoría interna o externa,
- qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos,
- si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o mediante contratación externa,
- qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados,
- si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y

  si sus conclusiones (seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el RGPD;

g) priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos;

h) asesorar sobre qué actividades de formación internas proporcionar al personal y a los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos;

i) intervenir en caso de reclamación ante las autoridades de protección de datos.

3 MODELOS ORGANIZATIVOS

3.1. Introducción

Dado que no existe una normativa específica que regule este aspecto, las organizaciones han implementado diversos modelos organizativos y relacionales para el Delegado de Protección de Datos (DPO), basándose en criterios variados y propios, como se puede ver reflejado en los resultados del último Estudio sobre el Nivel de Madurez y Cumplimiento del RGPD en España.

El modelo organizativo y relacional respecto a la posición del Delegado de Protección de Datos (DPO) dentro de la organización tiene un impacto considerable, ya que de ello dependerá en gran medida que este pueda cumplir con sus funciones de manera adecuada y conforme a los requisitos establecidos por el Reglamento de Protección de Datos en su sección 4. Esto incluye participar en tiempo y forma en todas las cuestiones relativas a protección de datos, contar con recursos suficientes y acceso a los datos personales y a las operaciones de tratamiento, actuar con independencia, evitar conflictos de intereses y rendir cuentas al más alto nivel jerárquico de la organización.

En este apartado se van a revisar los diferentes modelos más habituales, en cuanto a:

- Tipo de Delegado de Protección de Datos: Interno, Externo o Equipo Departamental.
- Modelos organizativos Posición en el organigrama.
- Modelo Relacional: Reporte y relación con el resto de la organización.

El RGPD no entra a regular, ni siquiera a recomendar, la forma en que las entidades públicas y privadas deban o puedan articular su Modelo Organizativo y Relacional en cuanto al DPO, circunstancia que otorga flexibilidad a cualquier entidad en la elección de su Modelo, dentro de su libertad de organización o de su esquema de la función pública, que podrá diferir de una entidad a otra y vendrá determinado, en gran medida, por las siguientes características:

- El tamaño de la organización y el tipo de actividades, procesos, productos y servicios
- Tipo de Actividades del Tratamiento llevadas a cabo por la entidad
- Preponderancia en sus actividades de las nuevas tecnologías y de la innovación
- Ubicaciones geográficas y transfronterizas (Local, europea o multinacional);
- La complejidad de los procesos y sus interacciones

En este mismo sentido, la AEPD en su informe jurídico 38/2023 ha determinado que el encuadramiento del DPO es una cuestión organizativa que puede adoptarse libremente por cualquier entidad -ajustándose en cualquier caso a la naturaleza asesora y supervisora de las funciones del DPO, con el único límite de que se garantice que la posición del DPO en la organización cumple con todos los requisitos establecidos en el artículo 38 del RGPD:

1. Participa en tiempo y forma en todas las cuestiones relativas a la protección de datos personales.
2. Dispone de recursos necesarios para el desempeño de sus funciones.
3. Desempeña sus funciones de manera independiente.
4. No es destituido ni sancionado por el desempeño de sus funciones.
5. Rinde cuentas al más alto nivel jerárquico de la organización.

Las organizaciones deberían esperar un mayor escrutinio e investigación de la AEPD en los próximos años respecto a la posición del DPO. Por este motivo, se recomienda tener en cuenta las necesidades y capacidades de cada entidad para optar por el modelo que mejor se ajuste a ella, con el objetivo de garantizar que la función del DPO se incardina de manera adecuada dentro de la organización. Una vez se determinen con claridad todas estas cuestiones, las entidades deben especificar claramente dentro de sus procedimientos organizativos, preferiblemente a través de un Régimen Interno del DPO o del contrato de prestación de servicios, en caso de ser externo, las cuestiones más importantes del Modelo Organizativo y Relacional del DPO:

- Tipo de DPO
- Ubicación y posición adecuada dentro de la Organización
- Nivel de reporte a la alta Dirección, procedimientos y vías de comunicación
- Procedimientos operativos de relación con otras áreas de la compañía
- Modelo de gobierno de privacidad, identificando los diferentes roles y responsabilidades en materia de protección de datos

En este mismo sentido, el Comité Europeo de Protección de Datos ha establecido una seria de recomendaciones y puntos de atención en torno a la figura del DPO[5], tanto del sector público como del privado, que las organizaciones deben tener en cuenta con independencia de cuál sea su modelo organizativo y relacional:

- Adoptar estándares, políticas internas y mejores prácticas que permitan acreditar el cumplimiento de las obligaciones del DPO en el modelo adoptado
- Asignación clara de cuáles son sus funciones internas, en particular que no tenga atribuidas otras tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos, circunstancia que afectaría a su independencia funcional.
- Fomentar su rol dentro de la organización y su participación en todas las cuestiones de protección de datos personales.
- Documentar el análisis respecto de la designación o no de un DPO, en especial si se concluye que su nombramiento no es obligatorio.
- Verificar los medios puestos a su disposición analizando, caso a caso, que medios resultan necesarios como, por ejemplo, el número de afectados cuyos datos son objeto de tratamiento en una organización
- Fomentar la formación de los DPO para que puedan mantener actualizados sus conocimientos y estar al día de las últimas novedades (normativa digital o de IA)

[5] *Coordinated Enforcement Action, Designation and Position of Data Protection Officers*

- Asegurarse de que puede cumplir con las tareas que tiene encomendadas por el RGPD
- Justificar que no asume responsabilidades que conlleven un eventual conflicto de interés ni se interfiere en su independencia, de manera especial cuando desempeñe otras funciones dentro de la organización.

En este apartado se plasman diversas reflexiones sobre los diferentes tipos de DPO, así como el modelo relacional de la figura dentro de la organización. Todo ello bajo un prisma de respeto a los diferentes modelos que existen en las organizaciones, y siendo conscientes de que no concuerda un encaje puro y perfecto entre los requisitos regulatorios de la función y el modelo de las 3 líneas de defensa que tan extendido está en multitud de organizaciones.

3.2. Tipo de Delegado: DPO Externo, Interno o Departamental

3.2.1. DPO Externo

El artículo 37 del RGPD permite el nombramiento de un Delegado de Protección de Datos externo a la organización, formando parte de un contrato de prestación de servicios con una persona física o jurídica. Esta es una opción residual, y en reducción según lo observado en el último Estudio sobre el Nivel de Madurez y Cumplimiento RGPD en España, con menos de un 3% de casos.

Según las Directrices sobre los Delegados de Protección de Datos del GT29 (ahora EDPB) esta opción permite que las tareas de DPO contratadas se presten por parte de un equipo del proveedor, pero en este caso, se exige que la totalidad de los miembros del equipo deberán cumplir todos los requisitos para ejercer las funciones de Delegado de Protección de Datos; además de que deberá existir un contacto principal designado para cumplir con el requisito de accesibilidad del DPO.

Este tipo de solución requiere, como ya hemos indicado, que exista un contrato de prestación de servicios, en el que se recomienda que, para evitar conflictos de intereses, evitar vacíos en cuanto a las funciones a cubrir y asegurar que se cumplen los requisitos del párrafo, se incluya al menos:

- Descripción detallada de las tareas asignadas al equipo del DPO externo.
- Responsabilidades de la propia organización tanto en esas tareas como en aquellas que se pudiesen asumir internamente.
- Designación de la persona física contacto principal y del gestor del proyecto de cara a la organización.
- Y por supuesto, un Encargo del Tratamiento puesto que el equipo del DPO accederá como encargado a información personal Responsabilidad del Cliente.

Tal como indica el EDPB (Comité Europeo de Protección de datos) en su informe de Enero del 2024 sobre la designación y posición del DPO, los responsables y encargados del tratamiento deben verificar cuidadosamente que el Delegado de Protección de Datos (DPO) disponga de recursos suficientes para ejercer adecuadamente sus funciones, y en algunos casos, cuando se emplea un DPO externo, esto puede requerir que los responsables y encargados del tratamiento verifiquen cuántos clientes tiene ese DPO, para asegurarse de que dispone de tiempo y capacidad suficientes para cumplir con las obligaciones pertinentes del RGPD.

La decisión de contratar un servicio externo de Delegado de Protección de Datos (DPO) depende en gran medida de la estrategia de gobierno del dato y de la gestión de la privacidad que se defina en la compañía, así como de su tamaño y capacidad para contar internamente con una persona que tenga el perfil adecuado para asumir el puesto.

Probablemente, este modelo no sea el más idóneo para grandes organizaciones que tienen la capacidad de establecer áreas de Protección de Datos y contar con un DPO adecuadamente formado. Un Delegado interno tendrá más facilidad para conocer la organización, su sector, y participar de forma efectiva en el día a día de la misma, lo cual puede ser un requisito en organizaciones con tratamientos numerosos, variados y cambiantes de datos personales. En cambio, en organizaciones más pequeñas, podría ser oportuna esta externalización ante la imposibilidad de contar internamente con un DPO adecuado.

PROS

- Reducción de costes de estructura al externalizar la función y por la capacidad de asignar recursos en función de necesidades puntuales, a través del contrato de servicio.
- Poder dotarse de profesionales con amplios conocimientos en todos los ámbitos necesarios en cuanto a Protección de Datos.
- Reducción del conflicto de intereses frente a otras funciones de la compañía.

CONTRAS

- Menor conocimiento de la organización y del sector de la misma.
- Dificultad para participar en todas las actividades relacionadas con el Tratamiento de Datos de la organización, cuando estas son muchas y complejas.
- Riesgo de falta de recursos por parte del proveedor en caso de que el mismo gestione demasiados clientes.

3.2.2. DPO Departamental (órgano colegiado o Comité)

Según la encuesta anteriormente citada, un porcentaje significativo de organizaciones ha optado por crear equipos de trabajo que asuman las funciones del DPO, representando un 30% de los casos. Sin embargo, esta opción está disminuyendo en favor de la designación de un DPO interno dedicado.

Aunque ni el Reglamento ni la LOPDGDD proporcionan una indicación clara en contra de que un órgano multipersonal pueda ser nombrado Delegado de Protección de Datos, la AEPD incluye en su Guía para Comunicar el DPO indicaciones sobre cómo comunicar un órgano colegiado o grupo de trabajo como tal. No obstante, surgen dudas razonables en este ámbito, ya que la redacción de la legislación parece estar orientada hacia una persona física y no un órgano multipersonal, especialmente considerando que esta posibilidad se establece específicamente para el caso de DPO externo. Además, las Directrices del GT29, al dar indicaciones para casos de grupos de trabajo, se refieren únicamente a DPO externos.

En todo caso, ante la falta clara de indicaciones en otro sentido, si se ha optado por esta solución parece que las indicaciones dadas por el GT29 para el caso de DPO externo son un punto de partida imprescindible en el caso de un equipo interdepartamental en lo que aplica:

- Todos sus miembros deben cumplir con los requisitos para ser DPO.
- Especificar claramente las funciones asignadas a cada miembro del equipo.
- Definir un punto único de contacto, tanto para la organización como para los interesados.
- Definir una persona única como punto de reporte con el Responsable.

Este modelo se fundamenta en el trabajo transversal dentro de la organización y puede ofrecer grandes ventajas en aquellas que ya tienen madurez en este tipo de organización, siempre y cuando las áreas adecuadas estén debidamente representadas. Se trata de un modelo que extiende a la privacidad el enfoque interdepartamental de la gestión de la seguridad, basado en Comités o Comisiones con atribuciones operativas que ya existían en muchas organizaciones.

PROS

- Asegura la transversalidad a lo largo de la organización si los miembros del comité han sido adecuadamente escogidos.
- Asegura que el órgano en su conjunto tenga todos los conocimientos y capacidades requeridos en un DPO.
- Optimización de Recursos: Cada departamento aporta recursos específicos, tanto técnicos como humanos, que pueden optimizarse en la gestión de la privacidad. Esta colaboración reduce la carga sobre el delegado de protección de datos y permite que la organización gestione mejor sus recursos en términos de privacidad y seguridad.
- Mejor Identificación y Gestión de Riesgos: Cada departamento maneja datos con distintos niveles de sensibilidad y diferentes procesos, por lo que contar con representantes de cada uno permite detectar riesgos específicos y adoptar medidas preventivas adecuadas para cada contexto.

CONTRAS

- Ciertas funciones del DPO son personales y requieren de una asignación de atribuciones dentro del Comité muy clara.
- Es más probable que existan conflictos de interés, pues cada área representada lleva los suyos; aunque su gestión es más sencilla por ser necesaria la toma de decisiones conjuntas.
- Desafíos en la Responsabilidad: Con múltiples responsables en temas de protección de datos, puede diluirse la claridad sobre quién toma decisiones finales o es responsable de determinadas áreas. Esto puede llevar a una falta de responsabilidad en casos de incumplimiento o incidentes.

3.2.3. DPO Interno

Según el Estudio sobre el Nivel de Madurez y Cumplimiento del RGPD en España, esta es la solución mayoritariamente adoptada (más del 55%), ya sea como una nueva función exclusiva definida o como una nueva atribución asignada a funciones y/o departamentos ya existentes en la organización.

PROS

- Un DPO interno está familiarizado con la estructura, cultura, procesos y sistemas de la organización, lo que facilita la identificación de riesgos específicos y la implementación de medidas adaptadas al contexto, y al formar parte de la organización, el DPO interno está siempre accesible para responder a dudas, incidentes o necesidades de formación, lo que permite una gestión ágil y continua de la privacidad,

CONTRAS

- aunque tiene el reto de tener que estar en formación continua para mantenerse al día con las regulaciones y prácticas de privacidad, lo cual puede ser demandante en términos de recursos.

3.3. Modelo Organizativo

3.3.1. Modelo I: DPO y CISO

Partiendo del modelo previo al RGPD en el que no existía en España ninguna figura semejante al DPO, pero sí la obligación de nombrar un Responsable de Seguridad, muchas empresas han ido optando por asignar este rol al CISO. Sin embargo, establecer ambas funciones a una misma persona puede generar retos, especialmente en cuanto a la posible existencia de un conflicto de intereses, dependiendo del tipo de CISO que exista en la organización.

Encontrar esta combinación de funciones no resulta extraño actualmente. De hecho, según puede observarse en el último Estudio sobre el nivel de madurez en la aplicación del Reglamento General de Protección de Datos de febrero de 2024, el 21% de los DPOs encuestados compaginan su cargo con el de CISO. En muchas organizaciones, son muchas las sinergias que se encuentran con este modelo desde un punto de vista operacional, cultural y de gestión de personas. Tanto la AEPD como recientemente la APDCAT se han pronunciado en sendos informes en relación con la coexistencia en una misma persona de ambas funciones destacando la importancia de la independencia del DPO para garantizar el cumplimiento del RGPD y la protección efectiva de los derechos de los interesados.

En su documento "2023 Coordinated Enforcement Action. Designation and Position of Data Protection Officers[6]", el EDPB incide en la idea del DPO multitarea señalando que un porcentaje significativo de DPO ocupan roles adicionales dentro de sus organizaciones, lo cual puede dar lugar a conflictos de intereses. Sólo el 45,82% de los DPOs trabaja a tiempo completo en sus funciones, mientras que el 33,97% está compartido entre varias organizaciones. Además, muchos DPOs también están involucrados en actividades que pueden chocar con su rol principal, comprometiendo su independencia.

La figura del CISO como tal no está regulada en la normativa con carácter general, siendo cierto que la normativa de ciberseguridad más actual sí contempla figuras de Responsable de Seguridad para entornos de infraestructuras críticas, entidades importantes y esenciales, etc. (por ejemplo. la Directiva NIS2). Las organizaciones, por tanto, ejercen su libertad empresarial para establecer un modelo de gobierno en materia de ciberseguridad que resulta muy variable y que da lugar a mucha casuística. El resultado es que existen CISOs con funciones de operación y mitigación de riesgos tecnológicos, otros tienen una labor más estratégica y de definición de políticas, unos están más cerca de la operación del negocio y otros una función de control y supervisión, unos trabajan entornos altamente regulados por una Autoridad de Control, y otros en mercados menos supervisados, unos con muchos recursos y diferentes perfiles en el equipo, y otros donde el departamento apenas es el propio CISO.

Por todo ello, **cada organización debe valorar la coherencia y el respeto de los principios mencionados anteriormente para recalar la figura de DPO y CISO en la misma persona o función.**

[6] *2023 Coordinated Enforcement Action. Designation and Position of Data Protection Officers*

El DPO debe estar implicado desde el inicio en la evaluación de licitud y proporcionalidad de los tratamientos de datos, antes incluso de que se definan las soluciones tecnológicas. Este es un punto clave en la protección de los derechos fundamentales de los interesados, que puede estar fuera del ámbito de un CISO cuya función esté centrada exclusivamente en las medidas de seguridad.

Tanto la Agencia Española de Protección de Datos (AEPD) en 2018 como la Autoritat Catalana de Protección de Dades (APDCAT) en 2024 han expresado opiniones similares sobre la concurrencia de las funciones de DPO y CISO en una misma persona. La AEPD resalta que la protección de datos es un derecho fundamental, mientras que la seguridad de la información es una obligación corporativa para garantizar un nivel adecuado de protección. Por lo tanto, debe existir una separación clara entre las dos funciones. Sin embargo, la AEPD admite que, excepcionalmente, en organizaciones pequeñas o con recursos limitados, podría permitirse que una persona asuma ambos roles, siempre que se cumplan una serie de requisitos clave.

Estos requisitos incluyen garantizar la independencia del DPO, evitar conflictos de intereses y establecer mecanismos organizativos claros para separar las responsabilidades además de que en dicha persona concurran los requisitos de formación y capacitación previstos en el RGPD. Tanto la AEPD como la APDCAT coinciden en la necesidad de garantizar la independencia del DPO, especialmente cuando este desempeña otras funciones dentro de la organización, como la de responsable de seguridad. La AEPD destaca que, en casos excepcionales en los que una persona asuma ambos roles, es fundamental adoptar "todas las medidas organizativas" necesarias, que deben estar "debidamente reflejadas en la Política de seguridad de la información", para asegurar que no haya conflicto de intereses y que el DPO mantenga su independencia.

Por su parte, la APDCAT refuerza esta idea al señalar que la designación del DPO debe estar "debidamente documentada" y que las medidas para garantizar su independencia se reflejen claramente en la política de seguridad de la organización. Además, la APDCAT va un paso más allá al recomendar la adopción de medidas internas específicas, como la definición explícita de los roles incompatibles con el del DPO, para prevenir posibles conflictos de interés.

Ambas autoridades enfatizan la necesidad de una estructura organizativa que garantice que el DPO pueda desempeñar sus funciones sin interferencias ni conflictos con otras responsabilidades que puedan comprometer su autonomía.

Tanto la AEPD como la APDCAT coinciden en señalar que la acumulación de los roles de DPO y CISO debe ser una medida excepcional, sujeta a una evaluación caso por caso.

La AEPD subraya que, en aquellos casos en los que no sea posible mantener una separación entre ambas funciones, es imprescindible documentar la designación del DPO, detallando los motivos que impiden la separación y las medidas adoptadas para asegurar su independencia, como podrían ser la utilización de direcciones de correo electrónico, presupuestos, recursos y reportes diferenciados e independientes.

3.3.2. Modelo II: DPO y Compliance

Por otra parte, un número importante de empresas han visto sinergias entre el puesto de Compliance y el de DPO, debido a que ambos puestos tienen como objetivo asegurar el cumplimiento normativo dentro de la organización, tanto en materia de protección de datos como en otras áreas de cumplimiento legal.

Desde la implementación del Reglamento General de Protección de Datos (RGPD), este modelo ha experimentado una evolución notable. Muchas organizaciones han visto beneficios al integrar la protección de datos en sus programas de compliance más amplios. Esta tendencia se ha observado en estudios que resaltan una mayor adopción de este modelo, sobre todo en pequeñas y medianas empresas (pymes) que carecen de recursos suficientes para mantener estas funciones separadas. Además, tanto la protección de datos como el compliance han adoptado un enfoque basado en la gestión de riesgos, lo que facilita la integración de estas funciones.

Sin embargo, es necesario tener en cuenta algunos aspectos a la hora de implementar este modelo:

- **Diferenciación de enfoques:** La labor del Compliance Officer se centra en la gestión de los riesgos que afectan a la organización desde un punto de vista regulatorio, mientras que el DPO se enfoca en la protección de los derechos y libertades de los interesados en materia de tratamiento de datos. Por ello, la especialización de cada rol es crucial para evitar posibles conflictos de interés y garantizar la eficacia de las funciones de control.

- **Capacitación adecuada:** Es esencial que la persona encargada de ambas funciones tenga la formación adecuada en ambos campos, tanto en el ámbito normativo como en los aspectos técnicos y legales.

- **Ubicación organizativa:** Este modelo puede permitir que el DPO se beneficie de la estructura organizativa del Compliance Officer, quien generalmente reporta directamente a la alta dirección. Este vínculo no solo puede favorecer la independencia del DPO, sino también aumentar su visibilidad dentro de la organización, promoviendo así una mayor integración de sus funciones.

- **Adecuación a los riesgos:** Este modelo es particularmente adecuado para organizaciones donde los riesgos de protección de datos están estrechamente relacionados con los procesos de negocio. La integración de ambos roles puede ser efectiva si se da prioridad a la evaluación de riesgos en función de las actividades empresariales y los tratamientos de datos. Sin embargo, l**a APD belga en su Decisión sustantiva 18/2020 advierte que la combinación de roles sólo puede considerarse adecuada si se implementan medidas sólidas para gestionar los conflictos de interés.** En caso contrario, como ocurrió en el caso analizado, la falta de segregación entre las responsabilidades del DPO y otros departamentos puede llevar a situaciones de autocontrol y falta de objetividad en la supervisión de los tratamientos de datos personales.

Las organizaciones deben llevar a cabo un análisis exhaustivo de la compatibilidad de las funciones de Delegado de Protección de Datos (DPO) y Compliance Officer, definiendo claramente el alcance y las responsabilidades de cada rol. Es crucial que se elabore un informe que detalle cómo se gestionarán y documentarán los posibles conflictos de interés. Esto puede incluir el establecimiento de políticas específicas para prevenir conflictos, un proceso riguroso de selección y formación de los candidatos, así como mecanismos de comunicación que permitan identificar cualquier vínculo que comprometa la imparcialidad en el desempeño de sus funciones.

3.3.3. Modelo III: DPO en área Jurídica

Otra posición muy común es asignar a un miembro del área Jurídica las funciones de Delegado de Protección de Datos. No obstante, es cierto que en los últimos años se mantiene la tendencia de no compatibilizar el cargo con otras funciones, lo que significa que casi la mitad de los DPO (46.81%) se dedican en exclusiva a sus funciones. Sin embargo, todavía un porcentaje significativo (17.02%) asume responsabilidades adicionales a las del DPO en el área jurídica.

Las sinergias en cuanto al conocimiento legal en materia de protección de datos parecen obvias, en particular en su función de asesoramiento en materia de protección de datos, siempre y cuando esto no suponga un conflicto de intereses, como por ejemplo, como podría ocurrir si el DPO tuviese una función ejecutiva dentro de la organización que implicara tomar decisiones sobre los fines y medios del tratamiento de datos personales, ya que el DPO debe evaluar, examinar y posiblemente criticar dicho procesamiento de forma independiente. Asimismo, en caso de desempeñar esa función ejecutiva, el DPO no podría supervisar el cumplimiento de la normativa sobre protección de datos, ya que este autocontrol contradiría la función del DPO como función independiente que debe garantizar dicho cumplimiento dentro de la organización.

Asimismo, otro posible conflicto de interés puede surgir cuando el DPO, directamente o como miembro del área jurídica represente al encargado o responsable ante los Tribunales en cuestiones relativas a la protección de los datos. Conflicto que el propio GT29 menciona en sus directrices, aunque sólo para el caso de DPO externo. Y lo mismo puede suceder a la hora de representar al encargado o responsable ante el órgano de control en cuestiones que no tengan que ver con su deber de colaboración, sino de defensa de este. En este sentido se ha pronunciado la Agencia Española de Protección de Datos, considerando que la presentación de alegaciones en representación del responsable del tratamiento es una función que va más allá del asesoramiento interno, implicando una defensa activa y una declaración de posición en un procedimiento sancionador, lo cual puede poner en riesgo la independencia del DPO y suponer un conflicto de intereses.

En cualquier caso, la determinación de la existencia de un conflicto de intereses debe efectuarse caso por caso, sobre la base de una apreciación del conjunto de las circunstancias pertinentes, en particular, de la estructura organizativa del responsable del tratamiento o de su encargado y a la luz de toda la normativa aplicable, incluidas las eventuales políticas de estos últimos. A tal fin, sería recomendable que aquellos

definieran las funciones del DPO para que éste pueda actuar con independencia dentro de la organización y se eviten posibles conflictos de intereses en relación con el ejercicio de sus funciones, por ejemplo, en un Estatuto del DPO aprobado por la alta dirección de la organización o una "engagement letter". En este sentido, la lista de funciones del DPO no es exhaustiva, por tanto, nada impide que el DPO asuma otras, como la de asesor jurídica, siempre y cuando el responsable o encargado del tratamiento se aseguren de que dichas funciones no puedan provocar un conflicto de intereses.

3.3.4. Modelo IV: Área independiente

Independientemente de la ubicación posterior en la jerarquía de la organización, continua la tendencia de años anteriores donde casi el 50% de DPOs se identifican como un área independiente de las ya existentes en las organizaciones.

Este Modelo permite realmente definir desde el inicio la posición del DPO dentro de su organización, así como la forma de realizar sus funciones dentro de la misma. Aunque en todo caso su eficacia en cuanto a los requisitos de realización de estas funciones también va a depender mucho de la dependencia jerárquica y del nivel de reporte definido para el mismo.

En este Modelo no existen en principio conflictos de interés, pero requiere que la organización tenga la capacidad de dotarse de un área exclusiva en cuanto a recursos y capacidades del DPO.

4 MODELOS RELACIONAL: REPORTE Y RELACIÓN CON EL RESTO DE LA ORGANIZACIÓN

4.1.Reporte del DPO

El reporte del DPO al más alto nivel jerárquico es un elemento clave para garantizar que las decisiones estratégicas de la organización en materia de protección de datos se tomen en base a un conocimiento adecuado de los riesgos. De igual modo, ha de tenerse en cuenta que el reporte directo del DPO al más alto nivel jerárquico del responsable o encargado es un mandato legal establecido en el artículo 38.3 del RGPD, debiéndose, por tanto, facilitar esta labor al DPO.

Para que el reporte sea efectivo, debe cumplir ciertos principios y estructurarse de manera que permita una comprensión clara del estado de situación en cada periodo de reporte, los desafíos y las acciones a tomar por parte de la organización. No solo es importante qué se reporta, sino también cómo se lleva a cabo ese reporte, puesto que la forma en que se presenta la información puede determinar la eficacia con la que la alta dirección asimila y actúa sobre los riesgos y recomendaciones presentados por el DPO.

4.1.1. Objetivo del Reporte

El objetivo principal del reporte del DPO debe ser proporcionar a la alta dirección una visión integral sobre el estado de cumplimiento en materia de protección de datos, los riesgos detectados, las posibles medidas correctivas necesarias y los aspectos que requieran mayor atención dentro de la organización. Esto permite a la dirección evaluar el nivel de madurez del sistema de gestión de protección de datos de la organización y tomar decisiones informadas sobre cuestiones clave, tales como la asignación de recursos y la adecuada gestión de los riesgos.

El reporte del DPO debe poder lograr varios propósitos clave:

- Garantizar que la alta dirección esté al tanto del nivel de cumplimiento de la organización respecto de la legislación en materia de protección de datos, o cualquier otra legislación sectorial con impacto en materia de protección de

datos, o cualquier otra legislación sectorial con impacto en materia de protección de datos, en función de los entornos y países en los que opere la compañía. La alta dirección debe ser conocedora ya no solo del nivel de cumplimiento, sino de la consecución de objetivos y las posibles desviaciones, tanto a nivel cuantitativo como cualitativo

- El DPO debe asesorar a la alta dirección sobre los riesgos más relevantes asociados a los tratamientos de datos personales efectuados por la organización. Estos riesgos pueden incluir posibles brechas de seguridad, fallos en los controles internos, o riesgos derivados de procesos tecnológicos que puedan afectar a los derechos y libertades de los interesados, ya sean trabajadores, clientes, usuarios o cualquier otro tercero cuyos datos personales son tratados por la organización.

- Informar sobre cualquier brecha de seguridad de datos personales que haya ocurrido durante el período de referencia, informando de sus consecuencias para los interesados que se hayan visto afectados, las acciones tomadas para mitigar el impacto, y las medidas correctivas que sea necesario implementar para prevenir futuros incidentes similares.

- No basta con informar sobre el estado actual, el DPO debería ser capaz de presentar recomendaciones estratégicas para mejorar el cumplimiento y minimizar los riesgos, sin olvidar que, en última instancia, corresponde al responsable del tratamiento tomar las decisiones ejecutivas en materia de protección de datos; el DPO no puede ni debe tomar decisiones en nombre del responsable, ya que esto constituiría un claro conflicto de interés respecto de sus funciones.

4.1.2. Frecuencia del Reporte

La frecuencia con la que el DPO reporta a la alta dirección dependerá de varios factores, como el tamaño de la organización, la complejidad de los tratamientos de datos personales, el sector en el que opera, y el nivel de riesgo al que está expuesta. Generalmente, **se recomienda que el reporte sea periódico, con una frecuencia mínima anual,** si bien en ciertos contextos en los que los tratamientos de datos personales constituyen el core de la actividad de la compañía, podría ser necesario reducir dicha periodicidad con un carácter semestral o incluso trimestral. En organizaciones con altos volúmenes de datos personales o que operan en sectores de alto riesgo, como el sector financiero o sanitario, puede ser necesaria una mayor frecuencia en el reporte para con objeto de mantener a la alta dirección informada en todo momento sobre los riesgos en materia de protección de datos personales. En sectores menos expuestos o en empresas de menor tamaño, los reportes pueden ser menos frecuentes, pero siempre deben realizarse, al menos, de manera anual, para asegurar que la dirección esté al tanto del estado de la protección de datos.

Además de los reportes periódicos, el DPO debe estar preparado para realizar reportes extraordinarios cuando ocurran eventos significativos, como brechas de seguridad graves o cambios de índole normativo que requieran una respuesta inmediata de la organización (por ejemplo, el lanzamiento de unas nuevas directrices específicas por parte del Comité Europeo de Protección de datos o de cualquier Autoridad de Control).

4.1.3. Metodologías de Reporte

El DPO puede adoptar varios modelos para estructurar sus reportes, dependiendo de las necesidades de la organización y del tipo de información que sea más relevante para la alta dirección. Dentro de las distintas metodologías de reporte, el DPO debe elegir la que mejor se adapte a las necesidades de información a transmitir, así como a las características de la organización, siendo fundamental que el modelo seleccionado permita una comunicación clara y efectiva, facilitando a la alta dirección la toma de decisiones informadas. Además, el DPO debe considerar factores como la complejidad de los tratamientos de datos personales, la frecuencia de los reportes y el nivel de detalle requerido por la alta dirección a la hora de elegir uno u otro modelo a seguir. A continuación, se describen los modelos más comunes:

i. Reporte basado en indicadores clave de rendimiento (KPIs)

Un modelo basado en KPIs ofrece a la alta dirección una visión cuantitativa del estado de la protección de datos. Los KPIs permiten medir el rendimiento del sistema de gestión de protección de datos a lo largo del tiempo y ofrecen una visión clara de los progresos o retrocesos en ciertas áreas clave, siendo fundamental que estos no solo se limiten a cifras absolutas y se informe igualmente comparaciones con periodos anteriores que permitan identificar tendencias, consecución de objetivos, desviaciones, etc. En el apéndice 1 se exponen algunos de los KPIs más útiles que podrá aplicar un DPO para medir el nivel de cumplimiento de la organización.

Es recomendable para organizaciones más pequeñas o con menor complejidad en el tratamiento de datos, o cuando la alta dirección prefiere una visión rápida y precisa de las áreas clave del cumplimiento. Este modelo es muy útil en entornos con menor riesgo, donde los indicadores numéricos proporcionan suficiente información.

PROS

- Los KPIs proporcionan datos cuantitativos que permiten una evaluación objetiva del rendimiento del sistema de protección de datos.
- Facilitan el seguimiento de los avances o retrocesos a lo largo del tiempo, permitiendo identificar tendencias y áreas de mejora.
- Ofrecen una base sólida para la toma de decisiones estratégicas, ya que se basan en métricas concretas y verificables.

CONTRAS

- Los KPIs pueden no proporcionar suficiente contexto sobre las causas subyacentes de las desviaciones o la consecución de los objetivos marcados, lo que puede llevar a interpretaciones erróneas.
- Pueden centrarse demasiado en aspectos cuantitativos, dejando de lado factores cualitativos importantes que también afectan la protección de datos.
- La recopilación y el análisis de datos para los KPIs pueden requerir recursos significativos, tanto en términos de tiempo como de tecnología.

ii. Reporte basado en riesgos

En este modelo, el DPO organiza el reporte en función de los riesgos detectados, priorizando aquellos que presentan una amenaza más inmediata o significativa, tanto desde el punto de vista corporativo como en relación con los derechos y libertades de los interesados. Es común que la alta dirección se enfoque principalmente en los riesgos que puedan tener un impacto significativo en la organización, y no tanto en aquellos impactos que una actividad de tratamiento pueda suponer sobre los derechos y libertades de los interesados. No obstante, el DPO debe ser capaz de trasladar claramente que los riesgos que afecten de forma severa a los derechos y libertades de los interesados, como el robo de identidad o el uso indebido de datos sensibles, podrían derivar en infracciones administrativas sancionables por la autoridad de control, sin perjuicio de las acciones legales y de reparación que pudieran emprender los afectados contra la organización.

Sin duda, una adecuada exposición y explicación sobre los riesgos a los que se enfrenta la organización será fundamental para que la alta dirección comprenda plenamente la magnitud y las posibles consecuencias en caso de que se materialicen, pudiendo implementar medidas de mitigación más efectivas y tomar decisiones informadas que protejan tanto a la organización como a los interesados.

Este tipo de reporte es recomendable en sectores de alto riesgo o donde el tratamiento de datos personales puede tener un impacto significativo sobre los derechos y libertades de los interesados. Por ejemplo, en organizaciones que manejan datos sensibles como empresas del sector sanitario, este modelo prioriza los riesgos críticos, permitiendo a la alta dirección focalizarse en las amenazas más urgentes.

PROS

- Permite a la alta dirección centrarse en los riesgos más críticos y tomar decisiones informadas para mitigarlos.
- Proporciona una visión clara y estructurada de los riesgos, sus impactos y las medidas de mitigación.

CONTRAS

- La alta dirección podría sentirse abrumada por la cantidad de información detallada sobre cada riesgo.
- Al centrarse en riesgos específicos, puede perderse una visión más holística del estado general de la protección de datos.

iii. Reporte basado en secciones de cumplimiento

Una metodología de reporte centrada en secciones de cumplimiento se basa en la revisión y evaluación sistemática de las áreas normativas claves que la organización debe cumplir en materia de protección de datos. Este tipo de reporte pone el foco en el nivel de cumplimiento que tiene la organización en puntos específicos del RGPD y otras normativas sectoriales.

Es ideal para organizaciones grandes con procesos complejos de protección de datos y donde la alta dirección requiere una visión completa y detallada de cada área del programa de cumplimiento. Por ejemplo, en una empresa multinacional que gestiona grandes volúmenes de datos de clientes, este modelo permite una evaluación exhaustiva y separada por áreas de cumplimiento.

El primer paso para estructurar un reporte basado en secciones de cumplimiento es identificar las áreas clave que deben revisarse. El reporte se organiza por secciones, cada una de las cuales cubre una de las áreas de cumplimiento identificadas.

A continuación, se describe cómo podría estructurarse cada sección:

1. **Descripción del Área de Cumplimiento:** Se explican brevemente las obligaciones legales que la organización debe cumplir en esa área específica. Por ejemplo, en la sección de "Transparencia y Derechos de los Interesados", se incluye un resumen de las obligaciones derivadas de los artículos 12 a 22 del RGPD.

2. **Estado de Cumplimiento:** Esta parte del reporte debe evaluar el grado de cumplimiento actual. El DPO puede utilizar un sistema de calificación (cumple, cumple parcialmente, no cumple) o una escala de porcentajes para indicar el nivel de conformidad en cada área.

3. **Acciones Correctivas Necesarias:** En caso de que se identifiquen incumplimientos o deficiencias, el reporte debería proponer acciones correctivas para alcanzar un grado de cumplimiento satisfactorio.

PROS

- Permite una mayor claridad sobre qué aspectos del cumplimiento concretos requieren atención, de forma que la alta dirección puede identificar fácilmente en qué áreas la organización está fallando y qué medidas deben ser tomadas.
- Permite una visión más holística de la situación de cumplimiento de la organización. En lugar de enfocarse solo en riesgos o KPIs aislados, este modelo ofrece una revisión exhaustiva de las obligaciones normativas clave.
- Dado que cada área se evalúa de manera individual, es fácil detectar cuáles son las secciones donde la organización no cumple con la normativa. Esto permite priorizar acciones correctivas y destinar los recursos de manera más eficiente.
- Esta metodología puede adaptarse a cualquier tipo de organización, independientemente de su tamaño o sector, ya que los aspectos de cumplimiento normativo aplicaran prácticamente por igual a cualquier responsable o encargado de tratamiento.

CONTRAS

- Al centrarse únicamente en el cumplimiento, esta metodología puede no prestar suficiente atención a la priorización de riesgos. Por ejemplo, una organización podría estar cumpliendo con las disposiciones normativas, pero enfrentarse a riesgos altos para los derechos y libertades de los interesados.
- La creación de un reporte detallado para cada área normativa puede generar una carga administrativa significativa para el DPO y su equipo. Además, este tipo de reporte puede volverse demasiado extenso y complejo, dificultando la toma de decisiones rápida por parte de la alta dirección.
- Sin indicadores numéricos claros que justifiquen las secciones de cumplimiento, puede ser difícil evaluar objetivamente el grado de cumplimiento y comparar el rendimiento a lo largo del tiempo. La ausencia de datos cuantitativos también puede limitar la capacidad de la alta dirección para tomar decisiones basadas en evidencia concreta.

iv. Reporte basado información combinada (cumplimiento, métricas, riesgos)

El modelo de reporte combinado reúne las fortalezas de los diferentes enfoques de reporte previamente descritos, integrando secciones estructuradas de cumplimiento normativo, indicadores clave de rendimiento (KPIs) y un análisis detallado de riesgos.

Mediante este enfoque híbrido se proporciona una visión integral sobre el estado de la protección de datos personales de la organización a la alta dirección, garantizando que los responsables puedan tomar decisiones informadas basadas tanto en métricas objetivas como en un análisis cualitativo y de riesgos, minimizando las limitaciones de los modelos individuales.

Es adecuado para organizaciones que requieren una visión integral que combine el análisis de riesgos, métricas cuantitativas y una evaluación cualitativa de áreas clave de protección de datos, siendo especialmente útil en empresas grandes con un alto volumen de actividades de tratamiento de datos personales.

a. **Resumen Ejecutivo:** este apartado es fundamental para proporcionar una visión clara y concisa a los miembros de la alta dirección que pueden no estar interesados en los detalles operativos, pero requieren un entendimiento general para la toma de decisiones rápidas y efectivas. Debe recoger un resumen de los principales riesgos de cumplimiento a los que se enfrenta la organización, las medidas que requieren una implantación inmediata, así como una selección de los KPIs más relevantes del periodo de reporte.

b. **Indicadores Clave de Rendimiento (KPIs):** en esta sección, se presentarán los principales indicadores de rendimiento relacionados con la protección de datos personales. Para evitar la sobrecarga de datos, es esencial priorizar aquellos KPIs que tienen un impacto directo en la gestión de riesgos y en la mejora continua del sistema.

c. **Riesgos actuales:** en este apartado, el DPO podría debería exponer los principales riesgos a los que se enfrenta la organización, tanto desde el punto de vista corporativo como en relación con los derechos y libertades de los interesados. Una adecuada exposición y explicación sobre los riesgos a los que se enfrenta la organización será fundamental para que la alta dirección comprenda plenamente la magnitud y las posibles consecuencias en caso de que se materialicen, pudiendo implementar medidas de mitigación más efectivas y tomar decisiones informadas que protejan tanto a la organización como a los interesados.

d. **Información sobre el estado de cumplimiento:** Como se ha explicado anteriormente, el reporte por bloques de cumplimiento se basa en la revisión y evaluación sistemática de las áreas normativas claves que la organización debe cumplir en materia de protección de datos. Esta sección del reporte debe poner el foco en el nivel de cumplimiento que tiene la organización en puntos específicos del RGPD y otras normativas sectoriales que sean de aplicación y que tengan impacto en materia de protección de datos.

La elección del modelo de reporte que el DPO utilice dependerá de varios factores clave dentro del contexto de la organización y las características específicas del tratamiento de datos personales. El DPO deberá considerar aspectos como el tipo de datos tratados, el tamaño de la organización, los recursos disponibles, la estructura jerárquica y las necesidades de la alta dirección para seleccionar la metodología que mejor facilite la toma de decisiones informadas y el cumplimiento normativo.

4.1.4. Factores que Influyen en la Elección de la Metodología

1. **Tipo de organización y sector:** empresas con altos volúmenes de datos sensibles (como las del sector sociosanitario) pueden beneficiarse más de un reporte basado en análisis de riesgos, ya que la gestión adecuada de los riesgos que afectan los derechos de los interesados es crucial en estos sectores. En organizaciones de menor tamaño o con datos menos críticos, un reporte basado en KPIs puede ser suficiente para ofrecer una visión clara de cumplimiento sin sobrecargar de información a la alta dirección.

2. **Complejidad de los tratamientos de datos:** en empresas con procesos complejos de tratamiento de datos que implican diversas áreas y sistemas, el reporte estructurado por secciones es ideal. Permite desglosar cada aspecto (auditorías, brechas de seguridad, formación, etc.), proporcionando un análisis profundo de cada área de tratamiento. En organizaciones con tratamientos más estandarizados, el uso de KPIs podría proporcionar una visión suficiente del desempeño, sin necesidad de un informe altamente detallado.

3. **Recursos disponibles:** si la organización tiene recursos tecnológicos y humanos limitados, puede optar por un modelo de KPIs, que es más fácil de gestionar y permite una evaluación rápida. En entornos con mayores recursos, el DPO podría implementar un modelo mixto o uno basado en riesgos para proporcionar una evaluación integral que requiere mayor esfuerzo en términos de análisis de riesgos y contextos.

4.1.5. Formas de comunicar el Reporte

El DPO puede optar por varias formas de comunicar la información a la alta dirección. Cada método tiene sus pros y contras, y la elección dependerá de las preferencias de la alta dirección, la cultura organizacional, y la naturaleza de la información que se debe presentar.

Reporte escrito detallado

Esta es una de las formas más tradicionales de reporte, en la que el DPO elabora un documento completo que incluye todos los detalles relevantes sobre el estado de la protección de datos en la organización.

PROS

- Permite que el DPO presente información detallada sobre cada aspecto de la protección de datos. La alta dirección puede revisar este informe a su propio ritmo y utilizarlo como una referencia a largo plazo.
- Proporciona un registro formal del estado del cumplimiento y los riesgos detectados en un momento específico. Esto es útil tanto para fines de auditoría como para medir el progreso a lo largo del tiempo.
- El DPO tiene la oportunidad de estructurar el informe de manera clara y lógica, proporcionando secciones separadas para cada tema relevante (cumplimiento, riesgos, incidentes, etc.).

CONTRAS

- Los informes detallados pueden ser extensos, lo que puede disuadir a la alta dirección de leerlos en su totalidad. En ocasiones, los miembros de la alta dirección pueden no tener tiempo para profundizar en todos los detalles y podrían pasar por alto aspectos críticos. En este sentido, se recomienda siempre incorporar un resumen ejecutivo que destaque los aspectos más críticos del reporte.
- Un reporte escrito no permite al DPO aclarar dudas o responder preguntas de manera inmediata, lo que podría llevar a malentendidos o falta de atención a ciertos puntos si no se da lugar a que el DPO pueda explicar ciertos aspectos del reporte que no hayan quedado claros.

Presentaciones gráficas y visuales

El uso de herramientas como gráficos, tablas y diagramas es una forma efectiva de transmitir información de manera concisa y visualmente atractiva. Estas presentaciones suelen ser más breves que los informes escritos y se centran en los puntos clave.

PROS

- Los gráficos y visuales permiten condensar grandes volúmenes de información en representaciones simples y fáciles de interpretar. Esto facilita que la alta dirección identifique rápidamente las áreas de mayor riesgo y las acciones recomendadas.
- Las presentaciones gráficas son más efectivas para destacar tendencias, comparaciones y métricas clave. Un gráfico bien diseñado puede tener un impacto más duradero que un párrafo de texto explicativo.
- Dado que las presentaciones gráficas suelen ser más breves, obligan al DPO a priorizar los puntos más importantes, lo que puede evitar la sobrecarga de cara a transmitir la información a la alta dirección.

CONTRAS

- **Aunque las presentaciones gráficas son útiles para proporcionar una visión general, pueden carecer del detalle necesario para que la alta dirección comprenda completamente los problemas más complejos.**
- **El éxito de una presentación gráfica depende de la habilidad del DPO para utilizar herramientas de visualización de datos de manera efectiva, lo que podría no ser siempre el caso.**
- **Aunque los gráficos y diagramas proporcionan una buena visión general, pueden necesitar explicaciones adicionales o contexto para que se comprendan completamente las implicaciones de los datos presentados.**

Exposición oral

Otra forma común de exponer el reporte es a través de una presentación oral durante una reunión del comité de dirección o un comité especializado en riesgos o cumplimiento. En este formato, el DPO tiene la oportunidad de exponer los puntos clave de su informe y responder preguntas en tiempo real.

PROS

- La exposición oral permite a la alta dirección interactuar con el DPO de manera directa. Esto facilita la resolución inmediata de dudas y la obtención de aclaraciones sobre aspectos específicos del reporte.
- El DPO tiene la oportunidad de enfatizar los puntos más importantes y persuadir a la alta dirección sobre la necesidad de actuar frente a ciertos riesgos. La presentación oral permite transmitir no solo datos, sino también el sentido de urgencia o prioridad.
- Durante la exposición, el DPO puede adaptar su presentación según la reacción de la alta dirección, enfocándose más en los temas que generan mayor interés o preocupación.

CONTRAS

- **Dependencia del tiempo asignado: El tiempo disponible para la exposición suele ser limitado, lo que puede hacer difícil presentar toda la información relevante. El DPO debe ser muy eficiente en la gestión del tiempo para asegurarse de que los puntos más importantes sean cubiertos.**
- **Aunque se puede ofrecer un resumen escrito después de la presentación, es posible que la alta dirección no tenga un documento detallado al que referirse en el futuro, lo que puede dificultar el seguimiento de los puntos discutidos.**

Presentación en el Consejo de Administración

En ciertas organizaciones, especialmente aquellas que operan en sectores altamente regulados, el DPO podría tener que reportar directamente al consejo de administración. Este tipo de reporte tiene un impacto significativo, ya que el consejo tiene una responsabilidad directa en la gestión de los riesgos de la organización.

PROS	CONTRAS
▪ El reporte directo al consejo de administración asegura que los temas relacionados con la protección de datos se traten al más alto nivel de la organización, siendo las decisiones tomadas en esta instancia las que tendrán un mayor peso estratégico y pueden resultar en cambios significativos en la organización. ▪ Involucrar al consejo de administración directamente en la supervisión de la protección de datos refuerza la responsabilidad y el compromiso de la organización con el cumplimiento normativo.	▪ No todas las organizaciones permiten que el DPO reporte directamente al consejo de administración. Además, en muchos casos, el tiempo que el DPO tiene para exponer su reporte ante el consejo puede ser extremadamente limitado. ▪ A nivel del consejo, es posible que los temas tratados sean de muy alto nivel y no se dé el seguimiento adecuado a los detalles más específicos del reporte del DPO.

Combinación de métodos

Al igual que se ha explicado en el epígrafe anterior, la mejor solución puede ser una combinación de varios métodos. El DPO puede presentar un informe escrito detallado con gráficos y tablas visuales para respaldar los puntos clave acompañándolo en paralelo de una presentación oral en una reunión con la alta dirección, donde resuma los puntos más importantes y responda a las posibles dudas y preguntas que puedan surgir. Este enfoque asegura que toda la información relevante esté disponible en diferentes formatos y que los detalles no se pierdan, a la vez que permite una interacción directa con la alta dirección.

Aunque el DPO tiene la flexibilidad para proponer un método de reporte que considere eficiente, **la última palabra sobre cómo y cuándo debe llevarse a cabo este proceso la tiene el responsable del tratamiento.** De acuerdo con el artículo 38 del RGPD, el responsable del tratamiento debe garantizar que el DPO pueda desempeñar adecuadamente sus funciones, lo que incluye proporcionarle acceso directo al más alto nivel jerárquico para la rendición de cuentas.

La forma de reportar dependerá, por tanto, de las necesidades y preferencias de la alta dirección, así como de la naturaleza y el riesgo asociado a los datos personales tratados. En cualquier caso, será deber del responsable del tratamiento facilitar los mecanismos necesarios para que el DPO pueda cumplir eficazmente con su labor de reporte.

4.1.6. Líneas a seguir en el reporte

Independientemente del modelo de reporte elegido, el DPO debe seguir una serie de pautas que aseguren la efectividad de la comunicación con la alta dirección:

- El lenguaje del reporte debe ser **claro y comprensible** para toda la alta dirección, incluso para aquellos que no tienen conocimientos técnicos profundos en protección de datos. Los tecnicismos deben evitarse o, al menos, explicarse brevemente para no perder la atención del lector.

- Es fundamental **destacar los riesgos más significativos y las acciones más relevantes.** La alta dirección debe poder identificar rápidamente los asuntos críticos que requieren su atención. El reporte no debe ser una lista exhaustiva de todos los incidentes menores, sino una presentación de las cuestiones que pueden tener mayor impacto en materia de cumplimiento.

- De igual modo, es recomendable incorporar en el reporte los **potenciales impactos** que podrían afectar a la organización tanto desde una perspectiva legal (multas o sanciones) como desde una perspectiva reputacional. Además, el DPO debe ser capaz de presentar estos impactos en términos económicos o estratégicos para que la alta dirección pueda comprender las posibles consecuencias. No obstante, debe recordarse que el cumplimiento en materia de protección de datos no debe ceñirse únicamente a evitar multas o sanciones por parte del responsable o encargado del tratamiento, sino a adoptar una postura proactiva que integre la protección de datos como un valor añadido para la organización.

- El DPO no debería limitarse a describir los problemas so pena de que su rol acabe interpretándose como un obstaculizador, sino que debe **proponer soluciones específicas sin entrar en un conflicto de interés.** Estas recomendaciones deben ser prácticas y estar alineadas con las capacidades y recursos de la organización, si bien deberá ser el responsable del tratamiento quién tome la decisión informada a la hora de implementar un plan de acción concreto o adoptar una medida específica.

- Es clave que el DPO enfatice que la protección de datos es una **responsabilidad compartida dentro de la organización.** Si bien el DPO juega un papel clave en la supervisión y asesoramiento, la implementación efectiva de las políticas y medidas en materia de protección de datos requerirán la colaboración de todos los departamentos involucrados en el tratamiento de datos personales, desde TI hasta recursos humanos y marketing.

4.1.7. Relación con otras áreas de la Organización

El DPO es una figura clave en el cumplimiento de la normativa de protección de datos personales dentro de una organización. Por ello, es fundamental que sea capaz de integrarse adecuadamente en la estructura organizativa, colaborando con diferentes áreas y generando sinergias que favorezcan un correcto desempeño de sus funciones. la colaboración de todos los departamentos involucrados en el tratamiento de datos personales, desde TI hasta recursos humanos y marketing.

El éxito del DPO no depende exclusivamente de sus conocimientos técnicos sobre la legislación, sino también de sus habilidades (también conocidas como *softskills*) para comunicar, influir y coordinarse con otros departamentos clave, especialmente aquellos que tengan un impacto o relación más directa con las actividades de tratamiento de datos personales. La relación que construya con cada área de la organización puede marcar la diferencia entre una implementación mecánica y una verdadera integración de una adecuada cultura de protección de datos personales en la operativa diaria de la organización.

4.1.8. Recursos Humanos (RR.HH)

El departamento de Recursos Humanos es una de las áreas más críticas con las que deberá colaborar el DPO, dado que será habitual el manejo de grandes cantidades de datos personales de empleados, candidatos y exempleados, entre los que se encontrarán normalmente datos muy sensibles (certificados de discapacidad, datos de salud, datos de nómina etc.). En ocasiones, el DPO podrá encontrarse con resistencias y retos importantes en esta área, especialmente en materia de conservación de datos personales.

4.1.9. Departamento de TI (Tecnología de la Información)

El DPO y el equipo de TI deben ser dos aliados naturales en la implementación de medidas de seguridad que protejan los datos personales, aunque a menudo pueden surgir desafíos relacionados con las prioridades. Mientras el DPO puede estar enfocado en el cumplimiento normativo, el departamento de TI puede tener como prioridad esencial la eficiencia operativa de los sistemas de información o la implementación de nuevas tecnologías. Estas diferencias pueden dificultar la colaboración si no se manejan adecuadamente.

El DPO necesita un conocimiento sólido de las tecnologías y sistemas utilizados en la organización, como los servidores, las bases de datos y las redes, para poder evaluar los riesgos asociados al tratamiento de datos personales. Pero más allá del conocimiento técnico, la clave de una colaboración eficaz radica en la habilidad del DPO para establecer una relación de confianza con los equipos de TI, asegurándose de que las soluciones técnicas sean compatibles y adecuadas con las exigencias del RGPD. Un reto frecuente será la capacidad del DPO para transmitir la necesidad de adoptar, desde el diseño de los sistemas de información, medidas de seguridad técnicas suficientes y adecuadas a los riesgos existentes en los tratamientos de datos personales que lleve a cabo la organización.

4.1.10. CISO o Responsable de Seguridad de la Información

En cuanto a la colaboración entre el DPO y el CISO (Chief Information Security Officer), esta relación es estratégica y debe estar basada en una coordinación fluida, ya que ambos roles comparten la responsabilidad de proteger los datos de la organización, aunque desde perspectivas diferentes. A pesar de las evidentes sinergias, el DPO se enfoca en asegurar que el tratamiento de datos personales sea legal y respetuoso con los derechos de las personas, mientras que el CISO se concentra en la implementación de medidas de seguridad técnicas y organizativas para prevenir vulnerabilidades y ataques que comprometan la información de la organización (entre la que se incluye la información de carácter personal). Uno de los desafíos más comunes es alinear las prioridades, dado que el CISO proporciona directrices encaminadas a garantizar la seguridad de la información, sean datos personales o simplemente información, mientras que las directrices que debe proporcionar el DPO están encaminadas a garantizar los derechos y libertades de las personas y no la seguridad de la información (considerando 77 RGPD).

4.1.11. Marketing y Ventas

Los departamentos de marketing y ventas suelen estar en el centro de la gestión de datos personales, utilizando herramientas como el CRM (Customer Relationship Management) o realizando campañas de email marketing. En este contexto, el DPO debe garantizar que las acciones del departamento se alineen con los requisitos de transparencia, concurrencia de bases legitimadoras adecuadas (consentimiento / interés legítimo) y ejercicio de derechos de los interesados.

Un desafío común que enfrenta el DPO en su relación con marketing es el equilibrio entre el cumplimiento normativo y las estrategias comerciales. Es lógico que el equipo de marketing este interesado en maximizar el uso de datos personales para personalizar las campañas y mejorar la conversión, debiendo el DPO procurar que dichos tratamientos se realicen dentro del marco legal, asesorando sobre la base legitimadora más adecuada, velando por que se obtengan los consentimientos necesarios y atendiendo a los interesados que ejerciten sus derechos, todo ello minimizando el impacto sobre las estrategias comerciales de la organización.

4.1.12. Área Legal

La colaboración entre el DPO y el departamento legal es probablemente una de las más fluidas, ya que ambos comparten el papel de asesor e informante

de riesgos, siendo una segunda línea de defensa de las compañías. Sin embargo, también pueden surgir tensiones cuando los enfoques difieren, ya que el departamento legal recibe directrices e instrucciones en el desempeño de sus funciones para alinear las estrategias legales con los objetivos del propio negocio, lo que en ocasiones puede colisionar con los intereses del DPO.

Una coordinación adecuada entre el DPO y el área legal será esencial para abordar temas como las brechas de seguridad, las transferencias internacionales de datos o la gestión de contratos con proveedores que impliquen el tratamiento de datos personales, colaborando para implementar cláusulas contractuales que protejan a la organización frente a posibles sanciones y, a su vez, cumplan con lo requerido por el RGPD.

4.1.13. Alta dirección

Como ya se ha profundizado en el capítulo previo, el apoyo de la alta dirección es esencial para que el DPO pueda cumplir con sus responsabilidades de manera efectiva. No obstante, uno de los mayores retos que enfrenta el DPO es trasladar a la dirección la importancia estratégica de la protección de datos, especialmente cuando no existe una percepción clara de los riesgos asociados a un mal manejo de la información de carácter personal.

El DPO debe ser capaz de articular claramente los beneficios de una política robusta de protección de datos, no solo en términos de cumplimiento normativo, sino también en relación a la confianza de los clientes, la reputación de la empresa y la minimización de riesgos financieros por posibles sanciones. Este proceso requiere una habilidad especial para influir y persuadir al más alto nivel jerárquico, mostrando que la inversión en protección de datos es una inversión en la sostenibilidad a largo plazo del negocio y un generador de valor corporativo.

5 SECTOR PÚBLICO

5. 1. Obligatoriedad de nombramiento de un DPO en el Sector Público

El RGPD en el artículo 37 dispone que el responsable y el encargado de un tratamiento realizado por una autoridad u organismo público tienen que designar un Delegado de Protección de Datos (en adelante, DPD), excepto los tribunales que actúen en ejercicio de su función judicial.

El criterio de obligatoriedad de designación del DPD deriva directamente del RGPD ya que en la LOPDGDD remite en este aspecto en el artículo 34 a lo previsto en dicho artículo 37 RGPD, sin matizar ni realizar especificación alguna en relación con las entidades o instituciones de carácter público.

Autoridad u organismo público son conceptos muy generales, se requiere de una mayor precisión; para ello acudimos al derecho nacional, en concreto, al artículo 2. Ámbito subjetivo de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, Ley 40/2015) en el que se indica:

1.

El Sector Público comprende:

a) La Administración General del Estado.

b) Las Administraciones de las Comunidades Autónomas.

c) Las Entidades que integran la Administración Local.

d) El sector público institucional.

2.

El Sector Público comprende:

a) Cualesquiera organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas.

b) Las entidades de derecho privado y vinculadas o dependientes de las Administraciones Públicas que quedarán a lo dispuesto en las normas de esta Ley que específicamente se refieran a las mismas, en particular a los principios previstos en el artículo 3, y en todo caso, cuando ejerzan potestades administrativas.

c) Las Universidades públicas.

3. **Tienen la consideración de Administraciones Públicas, la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local, así como los organismos públicos y entidades de derecho público previstos en la letra a) del apartado 2.**

Teniendo en cuenta este amplio y heterogéneo ámbito subjetivo de aplicación, la figura del DPD en estas instituciones y entidades deberá, en cualquier caso, adaptarse a la especial idiosincrasia de cada una de ellas, lo que no es tarea fácil dada su diversidad organizativa.

Al igual que en los demás ámbitos o sectores, la primera decisión deberá ser si se asume con medios propios la tarea o bien se externaliza.

5. 2. DPO externo

Al igual que en los demás ámbitos o sectores, la primera decisión deberá ser si se asume con medios propios la tarea o bien se externaliza. El artículo 37.6 del RGPD admite la posibilidad de externalización de la figura del DPO. En caso de externalización el DPO que podrá ser persona física o jurídica, se vinculará a la entidad pública mediante un contrato de servicios. Para la licitación, adjudicación y ejecución de estos contratos de servicios por las entidades públicas deberá estarse a lo previsto en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

El ámbito subjetivo de aplicación de esta norma incluye todo el sector público, e incluso puede afirmarse es de mayor amplitud que el expresado más arriba en relación con la obligación o incluso con la mera recomendación de contar con un DPO (vid. artículo 3 Ley 9/2017) Por otra parte, el contrato de servicios es contrato típico administrativo (vid. artículo 17 de esa misma norma).

Debe tenerse en cuenta que no se pueden trasladar a la organización de las entidades públicas los esquemas aplicables a organizaciones privadas y la prestación precisará de un adecuado conocimiento de las necesidades, organización y características propias de la entidad pública contratante, siempre además teniendo en cuenta que no pueden ser objeto de contratación las actuaciones y facultades que supongan ejercicio de autoridad (artículo 17 Ley 9/2017).

Por ello, en concepto de responsable del contrato (artículo 62 Ley 9/2017), deberá existir en la entidad pública una persona de enlace con la empresa contratada, con el fin de asegurar la correcta realización de la prestación pactada.

5. 3. Órgano colegiado

En el caso de que se opte por asumir la tarea con medios propios, es posible la designación de un único DPO para cada institución pública, pero no es aconsejable en los casos de grandes unidades u órganos con entidad y tareas claramente diferenciadas, por mucho que orgánicamente puedan depender de una única entidad. (En este sentido se pronunció el GT29 -actualmente extinto- en su análisis del DPO).

Ejemplo de lo expresado en el párrafo anterior es la Orden HFP/873/2021, de 29 de julio, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración digital del Ministerio de Hacienda y Función Pública.

La antedicha orden ministerial, en el artículo que regula la figura del DPO, expone que el DPO "es único para todo el Departamento sin perjuicio de la existencia de Delegados de Protección de Datos en los organismos públicos adscritos al Departamento y del nombramiento de coordinadores en todos los órganos superiores del Departamento y en la Intervención General de la Administración del Estado".

Nada obsta para que la función de DPO sea asumida por un órgano colegiado. Estos órganos colegiados tienen como regulación básica para la mayor parte de las entidades públicas la recogida en los artículos 15 a 24 de la Ley 40/2015. En estos casos deberá realizarse una clara asignación interna de tareas y responsabilidades, lo que deberá estar adecuadamente recogido en acuerdo de creación y en sus normas de funcionamiento.

El Centro Criptológico Nacional en la Guía CCN-STIC sobre Responsabilidades y Funciones en el ámbito del Esquema Nacional de Seguridad, establece que organizaciones de tamaño significativo pueden existir ciertos órganos o comités que puedan colaborar en la seguridad de la entidad, ya sea física, de la información, de protección de datos o de todas ellas. Entre los que señala como más habituales el Comité de Seguridad Corporativa, el Comité de Seguridad de la Información y el Comité de Protección de Datos.

En la referida Guía se dispone que "Cuando excepcionalmente pudiera constituirse un Comité conjunto de Seguridad de la Información-Protección de Datos, se deberá tener especial cuidado en analizar los posibles conflictos de intereses, muy especialmente en lo que se refiere al Delegado de Protección de Datos que, en el ejercicio de sus funciones, no podrá recibir instrucciones, debiendo responder al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios de tratamiento".

De todo lo anteriormente expuesto se deduce que, con independencia de la creación de un Comité, éste debe contar, entre otras, con la figura singularizada del Delegado de Protección de Datos.

5. 4. Modelo organizativo

En este sentido, la entidad debe organizar la seguridad comprometiendo a todos los miembros mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas en el marco normativo que afecta al desarrollo de las actividades y competencias de una administración pública, que comprende esencialmente su régimen jurídico, todas las normas jurídicas orientadas a la administración electrónica y su interoperabilidad, la seguridad de la información y los servicios que la manejan, la gobernanza y gestión del dato, su régimen de reutilización, transparencia, así como la protección de datos de naturaleza personal.

Dado que la seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos , teniendo en cuenta lo establecido en el Esquema Nacional de Seguridad, (Real Decreto 311/2002, de 3 de mayo) que contiene los principios básicos y requisitos mínimos necesarios para una protección adecuada de la

información tratada y los servicios prestados por parte de las entidades del sector público, y teniendo en cuenta a su vez, las pautas establecidas en la Guía CCN-STIC-801 "Responsabilidades y Funciones en el ENS", la administración pública, emprenderá las siguientes acciones:

- Designar roles de seguridad: Responsables de Servicios, Responsables de Información, Responsable de Seguridad de la Información, Responsable del Sistema y Delegado de Protección de Datos.

- Constituir un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se constituirá como un órgano colegiado y se denominará Comité de Seguridad y Protección de Datos. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

Los roles y órganos de seguridad y protección de datos serán los siguientes:

- Responsables de los Servicios y Responsables de la Información ENS: Los jefes y responsables de los diferentes órganos y unidades administrativas.

- Delegado de Protección de Datos: Comité de Seguridad y Protección de Datos, siendo interlocutor de la AEPD el Jefe de Servicio que se designe.

- Responsable de Seguridad de la Información ENS

- Responsable del Sistema ENS.

- Comité de Seguridad y Protección de Datos:

  o Presidente/a: Máximo representante de la entidad responsable del tratamiento

  o Secretario/a: Responsable de Seguridad

  o Vocales:

  - » Un responsable de la dirección de la entidad
  - » Un responsable de Administración Electrónica y Transparencia como responsable del tratamiento
  - » Un responsable del Gobierno del Dato como responsable de la información
  - » Responsable del sistema
  - » Persona designada como interlocultor/a con la AEPD

- El resto de Responsables de Información y los Servicios serán convocados por la presidencia en función de los asuntos a tratar.

5.5.1. Protección de datos y Seguridad de la Información en el Sector Público Hacia un nuevo modelo organizativo y relacional

En el caso de que se opte por asumir la tarea con medios propios, es posible la designación de un único DPO para cada institución pública, pero no es aconsejable en los casos de grandes unidades u órganos con entidad y tareas claramente diferenciadas, por mucho que orgánicamente puedan depender de una única entidad. (En este sentido se pronunció el GT29 -actualmente extinto- en su análisis del DPO).

5.5.1.1. Responsabilidad compartida en materia de seguridad y protección de datos en el Sector Público

No obstante la existencia de roles claramente definidos en el ámbito de la seguridad (Guía CCN-STIC-801) y la privacidad (RGPD-Delegado de protección de Datos), no cabe realizar una gestión independiente de la Protección de Datos Personales y de las medidas de adaptación al ENS; no son campos separables, constituyen un sistema único desde el punto de vista funcional y jurídico, por lo que la responsabilidad compartida entre Responsable de Seguridad y Delegado/a de Protección de datos en materia del establecimiento y determinación de las medidas de protección tiene sentido, dado que en el seno de las Administraciones Públicas, con carácter general, el objeto de la seguridad regulada en el ENS es la información del Sector Público, referida mayoritariamente a datos personales.

En este sentido, lo expuesto en la LOPDGDD de 5 de diciembre de 2018, en su disposición adicional primera (Medidas de seguridad en el ámbito del sector público) dispuso que:

1. EL ENS incluirá las medidas que deban implantarse en el caso de tratamiento de datos personales adaptando los criterios de determinación del riesgo en el tratamiento de datos y lo establecido en el art. 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica (Las Entidades Públicas como responsables de los tratamientos) deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el ENS, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

Posteriormente, en el art.3 del RD 311/2022, de 3 de mayo, por el que se regula el ENS, establece que cuando un sistema de información trate datos personales se aplicarán las normas que regulan la protección de datos personales (RGPD y LOPDGDD) y sus técnicas de protección (análisis de riesgos y evaluación de impacto en

PDP) y las medidas derivadas de ésta se impondrán a las previstas en el ENS, en caso de resultar agravadas respecto de las previstas en el ENS.

Por ello, y atendiendo a los principios de eficiencia, muchas administraciones públicas optan por la definición conjunta de la Política de Seguridad y Privacidad de Datos, así como por el establecimiento de un único Comité denominado Comité de Seguridad y Protección de Datos, donde ambas figuras, el Responsable de Seguridad y el Delegado de Protección trabajen de manera compartida.

En esta política deben establecerse los mecanismos concretos de resolución de controversias y conflictos, y así mismo deberán identificarse claramente a quién corresponden qué funciones, pudiendo determinar, además, aquellos puestos que serían incompatibles para el desempeño de estas funciones.

5.5.1.2. La comunicación electrónica entre entidades del Sector Público requiere de un trabajo colaborativo

La Ley 40/2015, en el apartado 2 de su artículo 156 define el ENS en los siguientes términos:

"El Esquema nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada."

En el mismo sentido, el art. 3 de la Ley 40/2015, dispone que las Administraciones Públicas se relacionarán entre sí y con sus órganos a través de medios electrónicos, que asegure la interoperabilidad y la seguridad de los sistemas y garantizarán la protección de los datos de carácter personal.

El mismo principio de actuación sistemática y colaborativa es el que contempla en el esquema conceptual previsto en la Guía STIC 801 del CCN-CERT para la organización de funciones y responsabilidades DPO, RSI y RS. Por otra parte, como puede verse, no se plantea jerarquía alguna en las relaciones entre RSI y DPO, cuya actividad se inscribe en un mismo marco de actuaciones concurrente.

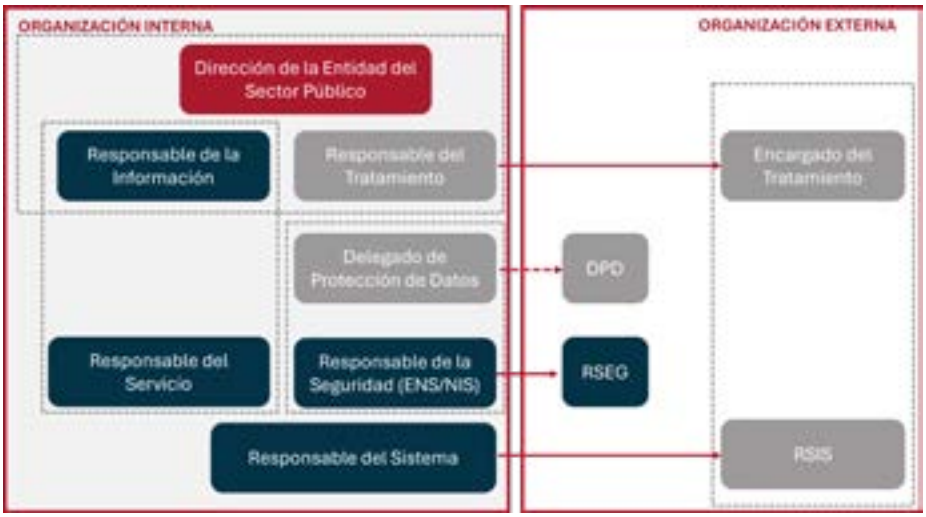

Imagen 1. Esquema conceptual de la Seguridad de la Información y la Protección de Datos

Muestra de la concurrencia lógica de responsabilidades es que la AEPD ha señalado la posibilidad de que la figura del Delegado de Protección de Datos coincida con el Responsable de Seguridad ENS en organizaciones que por tamaño y recursos no pudieran observar dicha separación. (Véase informe del Gabinete Jurídico de la Agencia de Protección de Datos[7]).

Delegado del Delegado de Protección de Datos y Delegado del Responsable de Seguridad

Tal y como se expresa en el desarrollo del ENS en aquellos sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesite de personal adicional para llevar a cabo las funciones de Responsable de Seguridad, cada organización podrá designar Responsables de Seguridad Delegados que delegará funciones, no responsabilidad. Cada Responsable de Seguridad Delegado mantendrá una dependencia funcional directa del Responsable de la Seguridad, a quién reportará. De igual forma, se determina la posibilidad de designar Responsables del Sistema Delegados.

Siguiendo con este razonamiento, y a la luz de las obligaciones del DPO para supervisar el cumplimiento del RGPD y otras normativas aplicables, incluyendo la asignación de responsabilidades, y ante la evidente falta de recursos con las que cuentan los DPO públicos, una de las formas en las que, ante la falta de una oficina de privacidad o un área encargada del apoyo requerido que necesita un DPO podrían llevarse a cabo, es la designación de competencias en materia de protección de datos a Responsables de Información y Servicios, o en su caso, el nombramiento de DPO Delegados que asuman las funciones encomendadas por éste en su área de competencia, como colaboradores especializados. Se subraya que lo que se delega son funciones, no responsabilidad.

5.5.1.3. Relación del DPO con otras áreas de responsabilidad en el Sector Público

En la Guía STIC 801 del CCN Cert se presenta un esquema que diferencia tres grandes bloques de responsabilidad:

1. La responsabilidad legal y la especificación de las necesidades o requisitos, que corresponde a la Dirección de la entidad y a los responsables del tratamiento de la información o servicio.

2. La supervisión que corresponde al Responsable de la Seguridad y al Delegado de Protección de Datos.

3. La operación del sistema de información, que corresponde al Responsable del Sistema.

[7] https://www.ismsforum.es/ficheros/descargas/independencia-dpd-responsable-de.pdf

Imagen 2. Bloques de responsabilidad

Dado el ecosistema tecnológico y normativo actual nacional y europeo, donde toda la norma en materia TIC, de seguridad, y protección de datos se encuentra armonizada e interdependiente, se procede a detallar la estrecha relación del DPO con las siguientes figuras de la Administración Pública, figuras tradicionales, o bien de nueva creación, de las que parte de su responsabilidad podrían ser asumidas inicialmente por el DPO.

El Delegado de Protección de Datos como "herramienta" de transparencia:

DPO y Responsable de Administración Electrónica/TI:

- Establecimiento de mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos, para tener el control de sus datos y el ejercicio de derechos, así como los procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD.
- Diseño de la seguridad, privacidad, accesibilidad y reutilización del dato por defecto.
- Coordinación de la obtención de datos de otras AAPP para fines distintos a la tramitación de procedimientos administrativos.
- Obtener un consentimiento jurídicamente válido con las debidas cautelas en el caso de menores.

DPO y Responsable de Archivo/Gestión Documental:

- Definición de los metadatos que determinen la existencia de datos de carácter personal.
- Gestión de los metadatos en publicación si pudieran identificar o hacer identificable a una persona física.

Todo ello conforme al Esquema Nacional de Interoperabilidad concretamente al esquema de metadatos para la gestión del documento electrónico (e-EMGDE).

DPO y Responsables de Contratación:

- Determinación de las condiciones tipo y clausulas a incluirse en los contratos de encargo de tratamiento.
- Necesidad de que sean los encargados del tratamiento con los que se haya contratado la prestación de determinados servicios los que colaboren en la atención a las solicitudes de los interesados. En estos casos, esa colaboración debe incluirse en los contratos de encargo de tratamiento.
- Criterios para valorar si los encargados con los que se hayan contratado o se vayan a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD. Para reforzar esta evaluación y dotar de mayor seguridad jurídica a las organizaciones, sería interesante contar con una certificación específica que acreditase el cumplimiento de los requisitos exigidos en los servicios de encargo de tratamiento en materia de protección de datos. Este tipo de certificación permitiría estandarizar buenas prácticas, facilitaría la selección de proveedores de servicios y fomentaría una mayor transparencia y confianza en el tratamiento de datos personales.
- Referente a la Gobernanza del Dato, incluir las cláusulas tipo para determinar las obligaciones relativas al acceso y reutilización de los conjuntos de datos que puedan generarse en la prestación del servicio o en el marco de un proyecto de investigación.

DPO y Responsable de información y servicios:

- Establecimiento del Registro de Actividades de Tratamiento
- Análisis de riesgo para los derechos y libertades de los ciudadanos de los tratamientos de datos que se desarrollen.
- Valoración de si los tratamientos que se realizan requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados y desarrollar dicha evaluación de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados

- Asunción por parte del Responsable de Información y Servicios, de la propiedad de los riesgos que existan sobre la información y los servicios de su competencia, así como de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad en materia de protección de datos y de disponibilidad en materia de seguridad.

DPO y Responsable de Seguridad:

- Necesidad de revisar las medidas de seguridad que se aplican a los tratamientos a la luz de los resultados del análisis de riesgo de los mismos. El RGPD exige que las medidas de seguridad se adecúen a las características de los tratamientos, sus riesgos, el contexto en que se desarrollan, el estado de la técnica y los costes.

- Necesidad de establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos y reaccionar ante ellas.

DPO y Responsable del Sistema:

- Colaborar en la realización de auditorías de cumplimiento de Seguridad y RGPD.

- Proponer por seguridad la suspensión del tratamiento de una cierta información.

- Según el ENS, el responsable de seguridad debe ser distinto del responsable del sistema y no debe existir una dependencia jerárquica entre ambos. Esto se debe a que el responsable de seguridad necesita tener la independencia necesaria para evaluar y asegurar la implementación de las medidas de seguridad sin conflictos de interés DPO y Responsable del Gobierno del Dato / Oficina del Dato.

En consonancia con el reglamento EU 2022/868 de 30 de mayo de 2022 relativo a la Gobernanza europea de datos y 2023/138 de 21 de diciembre de 2022 sobre datos de alto valor y modalidades de publicación y reutilización, y Ley 37/2007 de 16 de noviembre sobre reutilización de la información del Sector Público.

- Colaborar en los procesos de anonimización de datos personales

- Establecimiento de los requisitos de calidad del dato

- Dotación de medidas de seguridad y confianza para los espacios de datos del sector público, junto a las condiciones de acceso y reutilización.

- Colaboración en el gobierno del dato. Definición de mecanismos organizativos y técnicos dispuestos para obtener y tratar los datos conforme a los derechos de las personas, con licitud, calidad y de forma ética.

- Obtener consentimiento de los interesados para compartir los datos facilitados.

- Condiciones de preservación de datos históricos o su destrucción
- Coordinar el contenido del inventario de conjuntos de datos y fuentes de información con el RAT público.
- Colaborar en la valoración de la adecuación al derecho en base a su finalidad, de solicitudes de reutilización y acceso a conjuntos de datos.
- Determinar la limitación al tratamiento en conjuntos de datos reutilizables cuando así lo proceda el RGPD.
- Adecuación de la calidad e integridad de los datos para su posterior uso en sistemas IA garantizando el cumplimento normativo y los derechos de los interesados.

DPO y Responsable del Centro de Competencias de la IA:

- Informar y definir la base legal u obtener el consentimiento para la elaboración de perfiles y personalizar los servicios y otras finalidades de interés público.
- Indicar en el inventario de conjuntos de datos y fuentes de información la formación automatizada de actos administrativos u otras decisiones, indicando la naturaleza de dichos actos, los derechos de las personas que podrían verse afectados, especialmente en el caso de que los datos fueran inexactos o el algoritmo fuera inconsistente o presentara sesgos.
- Informar a los interesados de forma adaptativa en cada etapa del ciclo de vida de la IA en la que se esté realizando el tratamiento.
- En el caso de decisiones individuales automatizadas (art 22 RGPD), realizar un informe sobre su adecuación identificando posibles riesgos y proponiendo medidas de mitigación conforme a lo establecido en la Guía de Adecuación de la AEDP para tratamientos que incorporen IAs. Guía Adecuación AEPD.
- Realizar reevaluaciones continuas y auditorías de los tratamientos que incluyan IAs siguiendo las recomendaciones de la AEPD Requisitos auditorias IA. AEPD.

5.6. Perfil del DPO en el sector público

El RGPD establece en artículo 37.5 que el DPO "será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39".

Por su parte, el artículo 35 LOPD determina que el DPO podrá ser persona física o jurídica, y que para la demostración del cumplimiento de los requisitos de cualificación que se determinan en el artículo 37.5 del RGPD podrán utilizarse,

Entre otros, el mecanismo de certificación. Al efecto se determina que estos mecanismos de certificación tendrán particularmente en cuenta, por una parte, la obtención de una titulación universitaria que acredite conocimientos especializados en Derecho; por otra la práctica en materia de protección de datos.

El Considerando 97 del RGPD establece que, en el caso de una entidad pública, el responsable o encargado del tratamiento "debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial". Por el contrario, esta exigencia de especial conocimiento en Derecho y protección de datos se modula en el caso de entidades privadas, atendiendo a los criterios de cualidad (tipos de datos) y cantidad (a gran escala) del tratamiento.

Consecuentemente en el ámbito del sector público, parece que es lógico pensar que a las exigencias competenciales y profesionales predicables del DPO en general, se le deben añadir en forma obligada, algunas exigencias que vienen fijadas por el tipo específico de entidad al que nos referimos, lo que en primer lugar supone en todo caso e independientemente del tratamiento y de la cantidad de datos tratados, la exigencia de un perfil jurídico especializado. Así mismo, como afirma el GT29, es importante tener en cuenta que, en el caso de una autoridad u organismo público, el DPO deberá también poseer un conocimiento en la normativa específica aplicable a la organización, lo que supone un conocimiento sólido del ordenamiento jurídico-público y de los procedimientos de carácter administrativo, tanto en entorno convencional como en entorno digital.

Estamos por lo tanto diseñando un perfil curricular y profesional en el que se deben constatar conocimientos de alto nivel y titulación universitaria, normalmente a nivel MECES 3 (máster). Por otra parte, parece que, por el tipo de funciones, es adecuado pensar en un perfil de funcionario de carrera (artículo 9.2 del Estatuto Básico del Empleado Público Real Decreto Legislativo 5/2015, de 30 de octubre) lo que garantizaría su independencia, e inamovilidad, frente a otras figuras como los funcionarios interinos.

En principio, podría pensarse que no existe problema en admitir un perfil de empleado laboral (cabalmente, con contrato indefinido) para el DPO; si hemos admitido la posibilidad de que se externalice el DPO mediante un contrato de servicios, parece que entendemos que entre las funciones del DPO no está la del ejercicio de la autoridad. Ahora bien, analizadas las funciones del DPO, puede dar lugar a problemas en este aspecto es la función recogida en el artículo 37.1 de la LOPDGDD, (no se recoge en el RGPD).

Más allá de la función de colaboración con las autoridades de control que expresa el RGPD artículo 39 1.d), y que es reflejada en el artículo 37.2 de la LOP- DGDD, el artículo 37.1 LOPDGDD introduce la posibilidad de que el interesado presente "una reclamación previa" a la reclamación a presentar ante la AEPD. Esta reclamación será dirigida al DPO el cual deberá "comunicar en dos meses la decisión que se haya adoptado".

La aplicación de este procedimiento en el sector público, sobre todo en ámbito administrativo, nos lleva necesariamente hacia la materia de resolución de reclamaciones, procedimiento eminentemente administrativo que engarza con el concepto de ejercicio de autoridad.

Podría por lo tanto derivarse de la existencia de este procedimiento la interdicción para las entidades públicas, ya no solo de la externalización del DPO, sino también de la designación de un empleado cuya relación de empleo con la entidad sea de carácter laboral y no funcionarial.

Sin embargo, si analizamos la literalidad de la norma, también podemos llegar a una más flexible solución en los ámbitos contractual público y de categorización de tipo de empleado público. La norma en ningún momento dice que sea el DPO el que deba instruir o pronunciarse en relación con esa reclamación. No se otorga al DPO competencia en la resolución del asunto: la norma se limita a designar al DPO como "vía de comunicación" de la reclamación, tanto en el sentido de recibir la misma como de comunicar la resolución al interesado. Dicho, en otros términos, la LOPDGDD no se pronuncia ni sobre la naturaleza ni sobre la competencia de resolución de esta reclamación previa y deja margen de maniobra para incluir o excluir, según se estime conveniente por la propia entidad pública, al DPO de los procedimientos y actos administrativos que impliquen ejercicio de autoridad.

Trasladado esto a esquemas de derecho público, deberá analizarse en cada caso la competencia resolutoria de cada organización pública y actuar en consecuencia. Por ello, salvo los supuestos en los que se entienda que la competencia para instruir o resolver la reclamación recae en el DPO, podremos hablar de una intervención del DPO en este procedimiento de reclamación previa a nivel de informe, pero no de ejercicio de autoridad, dado con ello entrada tanto a la contratación externa como a la relación laboral.

En cualquier caso, lo lógico es que el puesto de trabajo se encuentre en el grupo de clasificación profesional A1, para funcionarios o asimilado en caso de laborales (artículos 76 y 77 del Estatuto Básico del Empleado Público Real Decreto Legislativo 5/2015, de 30 de octubre) siendo lo adecuado la exigencia de conocimientos en determinadas competencias generales y específicas. En el sector público, las competencias específicas del DPO so las mismas que las ya comentadas para el DPO en el ámbito privado. La especialidad en este caso se encuentra en las competencias generales exigibles.

El DPO de sector público, deberá de tener competencias generales a nivel especializado en derecho público, es decir, tener profundos conocimientos de las regulaciones aplicables al sector público en general y regulaciones aplicables específicamente al tipo de entidad pública. Además, deberá tener conocimiento sobre las tecnologías digitales en su concreta aplicación a las entidades y administraciones públicas. En este sentido, se precisa un conocimiento de las tecnologías digitales, no a nivel profundo y técnico, sino desde la perspectiva de su interacción con el sistema de protección de datos personales, y a su vez, como elemento estratégico para obtener un sistema de seguridad de los datos fiable e íntegro. Es de entender que los técnicos encargados del sistema de seguridad deberán interactuar eficazmente con el DPO en este ámbito.

Por último, simplemente constatar que, dependiendo de la actividad, podrá pensarse en un DPO con dedicación parcial o completa, debiendo en el primer caso afectar el nombramiento, necesariamente, a la distribución de las tareas compartidas, evitando en todo caso, tanto el conflicto de interés como la prevalencia de una de las dos tareas sobre la otra en tal medida que comprometa la atención adecuada de las funciones de DPO.

6 GOBIERNO DE LA PRIVACIDAD

6. 1. Deberes y Responsabilidades del Gobierno de la Protección de Datos

De conformidad con lo establecido en el RGPD, las entidades públicas y privadas deberán establecer las políticas y procedimientos adecuados para garantizar que tanto la empresa, como sus directivos, empleados y terceros cumplen con el marco normativo aplicable.

"La responsabilidad ante los incumplimientos e infracciones que prevé el RPGD recae en todo caso sobre el más alto nivel jerárquico en la organización: el Consejo de Administración y cualquier otro órgano en que se haya delegado oficialmente funciones de administración y dirección, como puede ser las Comisiones del Consejo, Consejero Delegado o el Presidente Ejecutivo."

Sin embargo, en organizaciones de cierto tamaño, puede resultar ingestionable que estos cargos puedan estar continuamente supervisando que los procesos de protección de datos están depurados y en efectivo funcionamiento y que las medidas son adecuadas; y tampoco es probable que estas figuras de alta responsabilidad reúnan el conocimiento especializado necesario para saber cómo o qué decisiones tomar ante ciertas actividades de tratamiento.

Por ello, para cumplir con la obligación de accountability, el RGPD propone la definición de un modelo de gobierno de la privacidad claro y documentado en la organización, que permita acreditar que, manteniendo su papel como el más alto nivel jerárquico en la organización (en la toma de decisiones y siendo quien debe recibir el reporte constante), otros equipos especializados y órganos intermedios hagan un seguimiento más inmediato y pongan en marcha de forma efectiva la gestión de la privacidad que en cada caso se determine. **Más allá de regular los casos en que existe una obligación expresa de designar un Delegado de Protección de Datos, el RGPD da libertad a las organizaciones para que establezcan el modelo de gobierno que consideren más adecuado**, siempre que, eso sí, les permita cumplir con las obligaciones que en virtud de estas normas les son de aplicación como Responsables y/o Encargados del Tratamiento.

El Gobierno de la Protección de Datos debe demostrar su liderazgo y compromiso en el cumplimiento del RGPD a través de sus acciones, creando un entorno en el que los diferentes actores participen plenamente y en el que el sistema de gestión pueda funcionar de forma eficaz en sinergia con los objetivos de la organización, lo que incluye:

a. Establecer las directrices y objetivos de la organización, garantizando que se establezcan las políticas de protección de datos adecuadas, determinando la dirección estratégica de la organización;

b. Promover políticas y objetivos en todos los niveles de la organización para aumentar la conciencia y la participación;

c. Asegurar la integración de los requisitos de los sistemas de gestión de la protección de datos en los procesos de la organización;

d. Determinar la competencia necesaria del Delegado de Protección de Datos, comprometiendo su apoyo en sus funciones para contribuir a la eficacia del sistema de gestión de la protección de datos;

e. Garantizar que están disponibles los recursos necesarios para el sistema de gestión de la protección de datos, con unos presupuestos adecuados;

f. Comunicar la importancia de una buena gestión de la protección de datos y de conformidad con el RGPD, para que alcance los resultados previstos;

g. Asegurarse de que los requisitos de las partes interesadas (clientes, empleados, accionistas, autoridades de control, etc.) son una prioridad en todos los niveles de la organización;

h. Garantizar que los procesos y controles son implementados para ayudar a satisfacer los requisitos de las personas físicas afectadas;

i. Asegurarse de que las responsabilidades y autoridades para funciones pertinentes sean asignadas y comunicadas dentro de la organización;

j. Evaluar los riesgos de los tratamientos de datos personales;

6.2. Modelo de Gobierno de la Protección de Datos

El punto de partida para un modelo robusto es establecer una estructura organizativa que defina claramente los roles y las responsabilidades, asegurando que la protección de datos sea un componente integral en la toma de decisiones. Este modelo debe abarcar desde la alta dirección hasta las áreas operativas, asegurando que cada nivel de la organización esté alineado con los objetivos de protección de datos establecidos por la organización.

> ***"Un modelo de gobernanza efectivo no solo debe garantizar el cumplimiento normativo, sino también integrar la protección de datos en los procesos estratégicos y operacionales de la organización."***

A continuación, se propone un modelo de gobierno que se organiza en tres capas principales: gobierno, supervisión y control, y operación.

6.2.1. Capa de Gobierno

Este nivel es responsable de definir las políticas generales, aprobar el marco de control y establecer las directrices estratégicas en materia de protección de datos, lo que de forma habitual corresponderá a la alta dirección de la organización. Los elementos clave de esta capa incluyen:

- Fijar la estrategia de protección de datos de la organización.
- Aprobación de políticas y procedimientos de protección de datos que regulen la gestión de la protección de datos en la organización (SGIP).
- Definición del modelo de gobernanza: establecer los roles, responsabilidades y líneas de reporte dentro de la organización.

6.2.2. Capa de Supervisión y Control

La capa de supervisión y control es la encargada de vigilar y evaluar el cumplimiento de las políticas y procesos establecidos por la capa de gobierno. La capa de supervisión y control trabaja estrechamente con la capa operativa para asegurar que los procesos de negocio implementen correctamente las políticas y procedimientos en materia de protección de datos. Además, esta capa debe informar regularmente a la alta dirección sobre el nivel de cumplimiento, los riesgos identificados y las medidas correctivas adoptadas.

Dentro de esta capa, se encuentra como segunda línea de defensa el DPO o un equipo de privacidad

especializado, como responsable de supervisar el cumplimiento normativo, promoviendo una cultura de privacidad en la organización y asegurándose de que las unidades de negocio gestionen los riesgos de manera adecuada.

Por otro lado, y dentro de esta capa, se encontraría auditoría interna y externa, quienes evaluarán igualmente de manera independiente la eficacia del modelo de gobierno de protección de datos. Esta línea de defensa asegura que apliquen adecuadamente los controles establecidos y se tomen las medidas correctivas necesarias, cumpliendo con los objetivos de protección de datos marcados por la alta dirección.

En esta capa se mantiene y actualiza el cuadro de mando con los KPIs definidos por la capa de gobierno. Los informes generados a partir de estos indicadores permiten a la alta dirección evaluar el nivel de cumplimiento y tomar decisiones correctivas si es necesario.

6.2.3. Capa Operativa

La capa operativa (sistemas, procesos y operaciones, etc.) es la encargada de la ejecución de los procesos de privacidad en el día a día de la organización implementando las políticas y procedimientos establecidos por la organización para el tratamiento de datos personales. Aquí es donde los procesos de negocio se alinean directamente con los requisitos del RGPD, y donde se implementan las medidas técnicas y organizativas necesarias para proteger los datos personales.

Dentro de la capa operativa se enmarcarán las unidades de negocio y de apoyo (asesoría jurídica, compras, operaciones / IT, seguridad etc.), siendo la primera línea de defensa y los responsables de identificar, evaluar y controlar los riesgos en materia de privacidad. La capa operativa es supervisada directamente por la capa de supervisión y control, recibiendo directrices y reportando sobre su implementación.

6.2.4. Sistema de Gestión de la Información de Carácter Personal (SGIP)

Aunque el término SGIP no es un término estandarizado ni universalmente reconocido en el ámbito de la privacidad y la protección de datos, al menos no con un uso tan extendido como otros conceptos como SGSI (Sistema de Gestión de Seguridad de la Información), que está vinculado a normas internacionales como la ISO/IEC 27001:.

> *"Se puede definir el Sistema de Gestión de la Información Personal (SGIP) como el marco documental que rige la gobernanza de la privacidad de manera integral en la organización, estableciendo los principios, políticas, procedimientos y controles necesarios para garantizar el cumplimiento del RGPD y otras normativas aplicables en materia de protección de datos."*

> *"El SGIP se fundamenta en los principios de responsabilidad proactiva, gestión del riesgo y mejora continua, asegurando la integración de la privacidad en todos los procesos organizativos."*

Estos documentos incluyen desde la política global de protección de datos, que establece los principios y directrices generales, hasta procedimientos específicos como la gestión de brechas de seguridad, la auditoría interna de protección de datos y el ejercicio de derechos por parte de los titulares de los datos. Cada uno de estos componentes es esencial para garantizar la protección adecuada de la información personal y el cumplimiento de las normativas vigentes.

A continuación, se presenta una propuesta detallada de la estructura del SGIP. Es importante destacar que cada organización debe ajustar esta estructura según sus necesidades y particularidades específicas, asegurando así una implementación efectiva y personalizada del sistema.

1. Política Global de Protección de Datos Personales

Este documento debe establecer los principios fundamentales sobre los que se asienta la protección de datos personales en la organización. Define las obligaciones y responsabilidades de todos los actores involucrados en el tratamiento de los datos y asegura el compromiso de la organización con el cumplimiento normativo.

Existen versiones internas y públicas de esta política, lo que permite que la organización informe tanto a su personal como a sus clientes y socios comerciales sobre sus prácticas de protección de datos.

2. Auditoría de Protección de Datos

La auditoría es un proceso esencial para garantizar la eficacia del sistema de protección de datos. A través de auditorías periódicas, la organización puede identificar posibles fallos o áreas de mejora en sus prácticas de tratamiento de datos.

Este procedimiento debe establecer las directrices para la realización de auditorías internas, definiendo roles y responsabilidades, así como las metodologías a seguir durante el proceso de auditoría.

3. Gestión de Brechas de Seguridad

Este procedimiento describe el proceso que debe seguirse en caso de detectar una brecha de seguridad que afecte los datos personales, desde su identificación y análisis, hasta la notificación de la brecha a la autoridad de control y, en su caso, a los interesados, o al responsable del tratamiento en caso de sufrir una brecha como encargados.

Además, es recomendable que se definan los planes de respuesta, así como las metodologías y criterios que se utilizarán para evaluar el riesgo provocado por una brecha de seguridad.

4. Atención al Ejercicio de Derechos

Este procedimiento detalla el proceso a seguir para la gestión de las solicitudes de derechos de los interesados, estableciendo las responsabilidades y el proceso de respuesta adecuado para cada solicitud, el registro de evidencias etc.

5. Política de Formación

Esta política debe establecer la necesidad de formaciones periódicas sobre protección de datos para todos los empleados, la clasificación de acciones formativas, planificación, la metodología de impartición, roles y responsabilidades, indicadores etc.

6. Política de Conservación de Datos

Esta política definirá los plazos de conservación de los datos personales en función de la finalidad del tratamiento, los criterios y causas habilitantes para el bloqueo o supresión de datos personales, así como los mecanismos de supresión y bloqueo implementados por la organización.

7. Política de Privacidad desde el Diseño y por Defecto

Esta política refuerza la adopción del principio de "privacidad desde el diseño", garantizando que la protección de los datos personales se integre en cada proceso y tecnología desde su fase de planificación, estableciendo para ello el procedimiento a seguir ante nuevos proyectos o iniciativas que impliquen el tratamiento de datos personales.

8. Procedimiento de Análisis de Riesgos y EIPD

Este procedimiento debe establecer las líneas a la hora de identificar y gestionar riesgos en el tratamiento de datos personales, incluyendo la metodología establecida tanto para el análisis de riesgos como para la gestión integral de las EIPD, identificación de roles y responsabilidades, y cómo documentar y revisar estos procesos.

9. Política de control de la cadena de suministro

Este documento del SGIP abordará la relación con terceros, como proveedores y socios comerciales que pueden manejar o acceder a datos personales en nombre de la organización, estableciendo el proceso a seguir para la evaluación y homologación de encargados y subencargados del tratamiento, o el marco de auditorías periódicas a terceros claves.

10. Estructura Organizativa en Protección de Datos

Este documento describirá la estructura organizativa de la protección de datos dentro de la empresa, identificando claramente los roles, responsabilidades y funciones, estableciendo igualmente los flujos de reporte y la interacción entre los distintos departamentos para asegurar una gestión integrada y coordinada de los datos personales en toda la organización.

El SGIP no solo es un conjunto de políticas y procedimientos, sino que se convierte en una herramienta vital dentro del modelo de gobernanza de la protección de datos, al proporcionar un marco operativo claro y detallado que regula el tratamiento de la información personal.

La eficacia del SGIP dependerá en gran medida de su aprobación por parte de la alta dirección. En primer lugar, ello garantiza el compromiso y respaldo necesario desde los niveles más altos de la organización, lo cual es fundamental para la implementación efectiva y sostenida del sistema. Además, la aprobación de la alta dirección refuerza la cultura organizacional de cumplimiento y responsabilidad, enviando un mensaje claro a todos los empleados sobre la importancia de la protección de datos.

Por otro lado, el respaldo de la alta dirección es esencial para enfrentar y mitigar riesgos asociados con la gestión de datos personales, incluyendo posibles sanciones legales y daños a la reputación de la organización. Un SGIP aprobado y apoyado por la alta dirección demuestra a las partes interesadas, incluidos empleados, clientes, socios comerciales y reguladores, que la organización se toma en serio la protección de datos y está comprometida con el cumplimiento de lo establecido en la legislación aplicable.

6.2.5. Integración con otras Funciones de Cumplimiento

Un modelo de gobernanza efectivo no puede operar de manera aislada. Es vital que esté alineado con otras funciones clave de cumplimiento dentro de la organización, como la gestión de riesgos, la seguridad de la información y la auditoría interna.

1.

Seguridad de la Información

La colaboración entre el equipo de protección de datos y el área de seguridad de la información es esencial. Si bien ambas disciplinas tienen objetivos diferentes (deben trabajar de la mano para proteger los datos personales de forma integral).

Es clave establecer canales de comunicación regulares entre ambos equipos para gestionar incidentes de seguridad y asegurar que las políticas de seguridad de la información estén alineadas con las normativas de protección de datos. Por ejemplo, medidas como el cifrado de datos, la gestión de accesos y los controles de seguridad físicos y lógicos deben ser evaluados en conjunto

2.

Auditoría Interna y gestión de Riesgos

El área de auditoría interna, como tercera línea de defensa, juega un papel crítico en la supervisión y control de los mecanismos implementados. Al integrar la protección de datos en los programas de auditoría interna, se garantiza que los controles sobre el tratamiento de datos personales sean revisados periódicamente y se identifiquen posibles fallos o áreas de mejora.

Para ello, resulta muy útil integrar la evaluación de riesgos de protección de datos en la matriz de riesgos generales de la organización. Esto permitirá priorizar aquellos procesos que presentan mayor riesgo para la privacidad y destinar recursos a mitigarlos de forma efectiva.

3.

Compliance

La función de compliance (también segunda línea de defensa al igual que el DPO) es otra área con la que el modelo de protección de datos debe estar alineado. Muchas normativas, como las relacionadas con blanqueo de capitales, salud o servicios financieros, o la gestión de los canales internos de denuncias, tienen intersecciones con la protección de datos, lo que hace indispensable la cooperación entre estos equipos.

6.2.6. Formación y concienciación continua

Otro de los pilares del éxito de un modelo de gobernanza es garantizar que todos los empleados comprendan sus obligaciones en materia de protección de datos y las implementen en sus actividades diarias.

La formación debe estar adaptada a las necesidades de cada rol dentro de la organización, asegurando que cada departamento reciba formación que se ajuste a sus responsabilidades en relación con el tratamiento de datos personales. Los empleados de TI, por ejemplo, necesitan entender los riesgos tecnológicos y cómo proteger los datos en sus sistemas, mientras que el personal de marketing debe ser consciente de las reglas sobre el consentimiento y el uso de datos personales para campañas publicitarias.

De igual modo, la formación no debe ser un evento puntual, sino un proceso continuo que garantice que los empleados estén al tanto de los cambios normativos y tecnológicos que afectan la protección de datos. Esto incluye no solo cambios legislativos, sino también nuevos riesgos o tendencias tecnológicas, como la IA o el análisis masivo de datos. Por ello, es clave establecer un programa de formación continua con cursos obligatorios anuales y evaluaciones periódicas para medir el nivel de conocimiento del personal.

Como ya se ha expuesto, la protección de datos debe convertirse en parte de la cultura organizacional. Esto implica no solo formación técnica, sino también la concienciación sobre la importancia de la privacidad y la protección de los derechos de las personas físicas, por ejemplo, mediante campañas de sensibilización que utilicen ejemplos concretos de riesgos, promoviendo una política de "puertas abiertas" donde los empleados puedan plantear dudas o preocupaciones sobre la protección de datos.

6.2.7. Fomento de la cultura de privacidad

El modelo de gobernanza de la protección de datos no se debe limitar a estructuras y procesos formales. Su éxito depende en gran medida de una cultura de privacidad arraigada en toda la organización que promueva la conciencia y el compromiso de todos sus integrantes con la protección de los datos personales, más allá del mero cumplimiento normativo. Desde la alta dirección hasta los empleados de línea, todos deben comprender la importancia de proteger los datos personales y cómo esta protección contribuye al éxito y la reputación de la empresa.

Por ello es relevante incluir referencias a la protección de datos y la privacidad en la misión, visión y valores de la organización. Al hacerlo, se refuerza la idea de que la protección de datos es parte integral del negocio, no solo una obligación legal.

6.3. Nivel Estratégico – Política de Protección de Datos

Como resultado del punto anterior, los objetivos corporativos y del propio sistema de gestión deberán quedar formalizados en una política de protección de datos, establecida en el artículo 24 del RGPD, así como la necesidad de adoptar dicha política expresada en el Considerando 78, que demuestre el compromiso y liderazgo por parte de

la alta dirección de la organización para impulsar una cultura y gestión de datos proactiva y efectiva, así como una actuación conforme a la normativa vigente, mediante el establecimiento y la difusión de los principios, valores y compromisos de la organización en esta materia. Las políticas de protección de datos son normalmente documentos clave, de alto nivel que deben traducirse posteriormente en procedimientos, estándares y guías que ayuden al cumplimiento de dichos objetivos.

En este sentido, la implantación de una política de Protección de Datos constituye una parte fundamental del gobierno de la privacidad y establece el compromiso de la organización en tratar la información personal con pleno respeto de los derechos y libertades fundamentales de los afectados. La política debe cubrir a clientes, empleados, contratistas, socios y otras entidades que necesiten acceso ocasional a datos, y su contenido podrá modularse en función del nivel y el tipo de riesgo que presenten las activades de tratamiento que realice la organización.

A modo de ejemplo, el detalle, la solidez y la completitud de la política de una entidad que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado, será mayor que para para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles. De igual modo, la política debe ser un documento fácil de entender y de seguir por el personal de la organización, su implantación no debe ser compleja ni difícil y deberá ser revisada y actualizada de manera periódica:

La Política debe reconocer los principios de protección de datos y los derechos establecidos en el RGPD, y debe explicar de qué manera se pondrán en práctica con relación a los tratamientos realizados por la organización. Sin intención de presentar un detalle exhaustivo, a continuación, se recogen **algunos puntos que pueden formar parte de dicha política:**

1. **Transparencia**

Compromiso de proporcionar información clara y sencilla a los interesados respecto a las condiciones de los tratamientos que les afecten como en las respuestas a los ejercicios de derechos, con independencia de sus conocimientos en la materia. En el caso de recoger datos personales de menores u otros colectivos especiales, se deberá ajustar el contenido de la información a presentar para que sea entendible.

2. **Minimización**

Compromiso de aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad.

3. **Licitud, transparencia y lealtad**

Compromiso de tratar los datos personales de manera leal, lícita y transparente para el interesado.

4. **Legitimación**

Todo tratamiento de datos necesitará apoyarse en una base que lo legitime. (consentimiento, necesario para la ejecución de un contrato, cumplimiento de una obligación legal, proteger intereses vitales del interesado o de otras personas, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, o la satisfacción de intereses legítimos prevalentes).

5.

Exactitud

Compromiso de disponer de medidas razonables para que los datos se encuentren actualizados, se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan.

6.

Inventario de Actividades de Tratamiento

Compromiso de crear y mantener actualizado un registro de operaciones de tratamiento de datos personales por la organización, tanto como Responsable de Tratamiento, como Encargado del Tratamiento.

7.

Limitación del plazo de conservación

Compromiso de mantener la información personal de forma que no se permita la identificación de los interesados durante más tiempo del necesario para los fines del tratamiento de los datos personales -solo podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. .

8.

Derechos de los Interesados

Compromiso de permitir que los interesados puedan ejercitar los derechos de acceso, rectificación, supresión ("derecho al olvido"), oposición, portabilidad, limitación del tratamiento, y derecho de oposición a las decisiones automatizadas (incluyendo la elaboración de perfiles).

9.

Seguridad de los Tratamientos

Compromiso en determinar y establecer las medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo en función del estado de la técnica, los costes de aplicación y, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

10. **Transferencias Internacionales**

Compromiso de únicamente proceder a la transferencia internacional de datos fuera del Espacio Económico Europeo cuando se garantice un nivel de protección de datos adecuado conforme al régimen jurídico de la UE, de conformidad con las condiciones establecidas en el capítulo V del RGPD.

11. **Roles y Responsabilidades Internas**

La necesaria identificación de los principales roles con responsabilidades internas en el sistema de gestión de protección de datos.

12. **Revisiones y Auditorías**

Compromiso de realización de auditorías internas del sistema de gestión y revisión de la eficacia y eficiencia de este por parte de la dirección.

13. **Relaciones con Encargados del Tratamiento**

Deber de adoptar medidas apropiadas para la elección de los proveedores de servicios con acceso a datos personales, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme el RGPD (principio de responsabilidad activa). De la misma manera, las relaciones entre el responsable y el encargado deben formalizarse en un contrato o en un acto jurídico que vincule al encargado del tratamiento respecto a la organización.

14. **Análisis de Riesgo**

Obligación de adoptar las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados, realizando una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo.

15.

Protección de Datos desde el Diseño y por Defecto

Responsabilidad de la organización de pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento, un producto o servicio que implique un tratamiento de datos personales.

16.

Violaciones de Seguridad de los Datos

Compromiso de que cuando se produzca una brecha de los datos personales, se notificará a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados. En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos.

17.

Evaluación de Impacto en la Protección de Datos (EIPD)

Deber de realizar una EIPD con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados.

18.

Delegado de Protección de Datos

Responsabilidad de analizar si la entidad debe proceder al nombramiento de un DPO y, de manera especial, justificar los casos en los que no se deba proceder a su nombramiento obligatorio, de conformidad con el artículo 37 del RGPD.

19.

Tratamiento de Datos de Menores

Obligación de realizar esfuerzos razonables con el objetivo de adaptar el deber de información y la obtención de los consentimientos, así como las actividades de tratamiento que realice la entidad, cuando se traten datos de menores de catorce años.

20.

Formación y Concienciación

Compromiso de facilitar a los empleados una formación periódica de concienciación sobre la protección de datos personales. Esta formación es fundamental para garantizar que el personal conozca las políticas de la organización, la normativa y los requisitos legales que se aplican a su función diaria.

Finalmente, como en todo sistema de gestión, la política deberá ser aprobada por la alta dirección, comunicada dentro de la organización de manera segura y estar disponible para las partes interesadas dentro de su alcance, normalmente el personal de la organización. De igual modo, resultará necesario garantizar y poder demostrar que la política se ha implantado y se aplica de manera adecuada. El desarrollo de los diferentes contenidos del sistema de gestión deberá estar vinculado con esta política, llegando a conformar un conjunto de normativas de la organización.

6.4. Nivel Organizativo – Roles y Relaciones

En cuanto al Nivel Organizativo, entre las entidades los roles clave más comunes que podemos encontrar en la toma de decisiones de la gestión de la privacidad se encontrarían:

1.

Alta Dirección: el RGPD establece que es el responsable o encargado, y no el Delegado de Protección de Datos, quien está obligado a aplicar "medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento" (artículo 24.1). El cumplimiento de las normas en materia de protección de datos es responsabilidad corporativa del responsable del tratamiento.

La alta dirección (al nivel del consejo de administración) tiene un papel fundamental a la hora de posibilitar el desempeño efectivo de las tareas del DPO, tiene la obligación de apoyar de manera activa su labor y deberá estar informada de manera directa del consejo y recomendaciones del DPO.

Además, serán los encargados de impulsar la existencia de una cultura de cumplimiento de la normativa de protección de datos por medio del establecimiento y la difusión de los principios, valores y compromisos de la organización en dicha materia.

2. **Delegado de Protección de Datos (DPO):** El DPO es la piedra angular del cumplimiento de la normativa de protección de datos en las organizaciones y, por lo tanto, es el participante clave en el gobierno de la privacidad. En concreto, el DPO es el enlace entre la alta dirección y el sistema de gestión de protección de datos. A nivel de gobierno, el DPO debe reportar de manera directa a la alta dirección, pero también debe comunicarse y coordinarse con todas las partes interesadas de las diferentes Áreas de Negocio.

3. **Equipo del Delegado de Protección de Datos:** según el tamaño, estructura de la organización y la asignación del rol de Delegado de Protección de Datos, puede ser necesario que este disponga de un equipo de soporte para el desempeño de sus funciones. En esos casos, deben delimitarse con claridad la estructura interna del equipo y las tareas y responsabilidades de cada uno de sus miembros.

4. **Responsables de Protección de Datos por Áreas de Negocio:** son los responsables de asegurar que la política de protección de datos sea incorporada y gestionada apropiadamente en el alcance de sus funciones y actividades de negocio. Cuando las organizaciones tienen distintos departamentos clave que tratan datos personales, es frecuente encontrar que representantes globales/locales de estos, tienen asignadas funciones específicas de protección de datos.

5. **Responsable del Tratamiento:** Es la entidad que, al definir los fines y los medios del tratamiento es, en última instancia, la responsable del uso apropiado y de la seguridad de los datos personales durante todo el ciclo de vida del tratamiento**.**

6. **Encargado del Tratamiento: es la entidad que procesa los datos personales en nombre y por cuenta del responsable del tratamiento. Las actividades de tratamiento que realiza deben satisfacer las políticas, procedimientos, estándares y principios generales de privacidad establecidos por el Responsable del Tratamiento.**

Y entre los mecanismos de relación más habituales entre estos roles y entidades dentro de una organización, caben señalar los siguientes:

1. **Consejo de Administración:** El Delegado de Protección de Datos debe reportar los problemas clave relacionados con el cumplimiento de la normativa de protección de datos a la Alta Dirección de la organización. Reportar de manera directa al Consejo de Administración u otro órgano o comité de dirección es lo habitual cuando existen situaciones de especial relevancia, y al menos se deberá presentar un informe anual con las actividades del DPO.

2. **Otros Comités**: en función de la estructura, es frecuente encontrar ejemplos de interacción del Delegado de Protección de Datos con otros comités en diferentes ámbitos:
   - Comités Globales: Comité de control de riesgos y Cumplimiento, Seguridad de la Información, Legal, Ciberseguridad, etc.
   - País
   - Funciones Negocio

3. **Foros del Delegado de Protección de Datos:** es frecuente que el Delegado de Protección de Datos establezca un foro para coordinar el sistema de gestión de la privacidad con diferentes puntos de enlace con unidades de negocio o responsables de protección de datos por País.

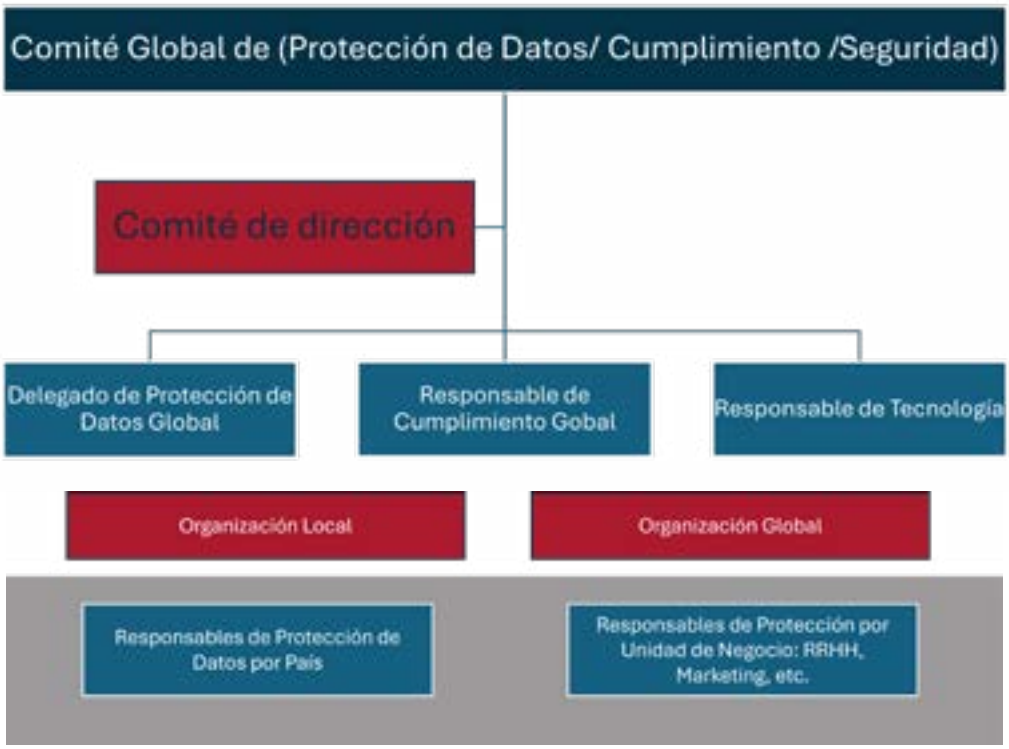

Imagen 5. Modelo de Gobierno de Privacidad – Multinacional

6.5. Problemas prácticos del Gobierno de la Protección de Datos

De lo visto hasta ahora, es evidente que la articulación del Gobierno de la Protección de Datos dentro de las organizaciones, tanto públicas como privadas, continúa enfrentando desafíos comunes con otros ámbitos de cumplimiento. Entre ellos se incluyen el encaje del Delegado de Protección de Datos, y su relación con figuras como el Compliance Officer o el CISO, en la integración de la estructura orgánica de la empresa, con líneas de reporte poco claras y órganos de gobierno que pueden ser disfuncionales. A esto último, se suma la incertidumbre sobre las nuevas funciones que debe de asumir el Delegado de Protección de Datos ante la entrada en vigor y su aplicación del Reglamento de Inteligencia Artificial.

Resultando importante resumir los desafíos relacionados con la implementación y gestión efectiva del modelo de gobierno de la protección de datos:

a) Cultura de protección de datos:

Uno de los mayores retos de los últimos años ha sido implementar la cultura de protección de datos en todas las organizaciones. El desafío al que se enfrentan las entidades públicas y privadas sujetas al cumplimiento del RGPD que, a través de sus actores principales en esta materia, tanto el Gobierno de la Protección de Datos como el Delegado de Protección de Datos, se traza en dos líneas, la primera, **extender la cultura de la protección de datos a toda la organización,** siendo consciente de que su éxito dependerá de la elección del modelo de gobierno que mejor se adapte a las características de cada entidad, pública y privada, y el apoyo que la alta dirección ofrezca al mismo; y la segunda, lograr **educar a todos los miembros de la organización en la cultura del cumplimiento de la protección de datos,** mediante programas de concienciación y una buena gestión de sus políticas en esta materia.

b) Apoyo e implicación de la alta dirección

Mucho se habla sobre reportar a la alta dirección, pero poco sobre el liderazgo que la misma debe de tener, proporcionando los recursos necesarios (financieros, humanos y tecnológicos) y liderar con el ejemplo para que la protección de datos se vea no solo como una obligación normativa, sino como un valor estratégico y añadido para la organización. Asegurando que se establezcan políticas eficaces, que se definan los roles, funciones e interrelaciones existentes entre las diferentes personas o equipos que tienen relación con el tratamiento de datos de carácter personal y que este modelo se comunique expresamente a toda la organización. Evitando de esta manera la indefinición de quién asume la responsabilidad en la gobernanza de la privacidad, quién toma las decisiones respecto a las políticas de protección de datos y quién asume los riesgos de su falta de cumplimiento.

> ***"El compromiso activo de la alta dirección es fundamental para el éxito del gobierno de la protección de datos, ya que su liderazgo y apoyo en la asignación de recursos, la definición de roles y la promoción de una cultura de cumplimiento permiten que la protección de datos se perciba como un valor estratégico y no solo como una obligación normativa. Sin este respaldo, los esfuerzos del DPO pueden verse limitados e incluso resultar ineficaces."***

La práctica demuestra que la falta de implicación de la alta dirección puede resultar en la percepción de la protección de datos como una tarea meramente burocrática, lo cual socava la adopción de buenas prácticas en toda la organización.

Resulta habitual que, en organizaciones más pequeñas el liderazgo y compromiso está menos presente y es donde el delegado de protección de datos suele tener más trabajo para sentar las bases del buen gobierno de la privacidad en la organización.

c) Establecimiento de directrices, responsabilidades y objetivos claros:

La falta de claridad en la asignación de funciones y responsabilidades en relación con los objetivos de la protección de datos puede llevar a una gestión ineficaz y a riesgos de incumplimiento. De una parte, deviene fundamental que las responsabilidades estén claramente definidas y comunicadas en toda la organización. Sin embargo, pese a que se definan muy bien los roles y responsabilidades, muchas organizaciones a menudo encuentran difícil convertir desde los principios de la protección de datos hasta los requisitos más complejos, en directrices estratégicas que se integren de forma efectiva con sus objetivos de negocio. Este desafío puede además generar tensiones entre el cumplimiento normativo, la vulneración de los derechos de las personas y otras prioridades estratégicas, lo que se traduce en políticas de protección de datos que no se implementan de manera uniforme o que no son entendidas por toda la organización. Es común que áreas como la de marketing, por poner un ejemplo, no consideren los principios fundamentales o requisitos básicos de la protección de datos, ya que perciben las exigencias normativas como un obstáculo para sus actividades principales y la agilidad del negocio.

> *"Es fundamental definir y comunicar de forma precisa los roles y responsabilidades en toda la organización, integrando los principios de protección de datos con los objetivos de negocio."*

La comunicación efectiva juega un papel fundamental para asegurar que toda la organización comprenda la importancia de la protección de datos. Sin embargo, los mensajes suelen no llegar a todos los niveles de forma adecuada. Resultando necesario adaptar la comunicación a las diferentes audiencias y roles dentro de la organización para lograr un impacto real.

Igualmente, en lo relativo a asignación de roles, en empresas pequeñas, es habitual que el DPO asuma muchas responsabilidades para maximizar los recursos, lo cual puede llevar a que su papel de supervisor de la privacidad entre en conflicto con otros roles operativos. En estos casos, la organización puede tener dificultades para asegurar que el DPO actúe con la imparcialidad necesaria, lo que plantea un reto en la gestión de su independencia y la evitación de conflictos de intereses.

d) Integración en los procesos operativos y asignación de recursos:

La implementación efectiva de los requisitos y obligaciones de protección de datos debe de hacerse en los procesos internos, esto puede chocar con la rigidez de algunos procesos tanto existentes como nuevos, por ello resulta habitual que se comunique al DPO, los cambios, modificaciones de los procesos del negocio para que se valore si se integran determinados controles en cumplimiento con la normativa actual y aplicable en materia de protección de datos. En la práctica habitual, hay todavía empresas que no realizan mapeos de datos en función a los procesos del negocio, puesto que todavía se tiene la estructura bajo ficheros de datos que suele ser más simple y sencilla de elaborar.

"La integración efectiva de la protección de datos en los procesos operativos requiere adaptar los controles a la normativa vigente, lo que puede verse limitado por la rigidez de ciertos procesos y la falta de comunicación con el DPO."

Por otro lado, la falta de recursos no solo afecta la implementación de medidas técnicas y organizativas, sino también la capacidad para llevar a cabo programas de formación, auditorías y evaluaciones de impacto. Como ya se ha visto en anteriores epígrafes, no es lo mismo tener un DPO externo, interno o todo un departamento de privacidad, el presupuesto destinado puede definir el alcance del modelo de gobierno o arquitectura de privacidad que se quiera desarrollar.

Una realidad común en pequeñas y medianas empresas, por ejemplo, es que tienen toda la documentación elaborada pero no está integrada en sus procesos, debido a la falta de cultura de cumplimiento en protección de datos y reforzada por la poca asignación de recursos.

e) Gestión, evaluación y documentación de los riesgos

En un entorno tan dinámico, los riesgos relativos a la protección de datos han cobrado gran protagonismo debido al incremento de ciberataques. La realización de evaluaciones periódicas ya sea desde análisis de riesgos básicos hasta valoraciones más completas como Evaluaciones de Impacto en Protección de Datos (EIPD) y la actualización de las medidas de seguridad, así como su implementación pueden llegar a convertirse en un desafío constante, especialmente en aquellas organizaciones con estructuras más complejas.

Los últimos años la implementación de medidas preventivas a través de protocolos ante incidentes y brechas de protección de datos son más que habituales y se han tornado en herramientas fundamentales. Aún en algunas organizaciones se puede apreciar el desconocimiento de este proceso previamente definido, por la falta de formación o capacitación al personal.

Finalmente, la falta de una adecuada gestión documental a nivel general y no sólo relativa a brechas de seguridad, puede llevar a deficiencias en el buen gobierno de la protección de datos de la entidad. No se trata de elaborar mucha documentación, pero sí que la que se elabore se haga con la finalidad de promover la eficacia, así como la mejora continua de la gobernanza de los datos.

"La gestión eficaz de la protección de datos requiere evaluaciones de riesgos periódicas, medidas preventivas ante incidentes y una adecuada documentación que promueva la mejora continua."

f) Funciones del DPO en materia de inteligencia artificial:

Con la reciente entrada en vigor del Reglamento de Inteligencia Artificial, las funciones del DPO deberán adaptarse para asumir los desafíos específicos asociados al uso de tecnologías de Inteligencia Artificial y que se han abordado también en el presente documento.

"El DPO debe adaptar sus funciones para abordar los riesgos de la inteligencia artificial, garantizando la protección de datos, la transparencia en decisiones automatizadas y el cumplimiento normativo durante todo el ciclo de vida de los sistemas."

De momento el DPO continuará presente en la evaluación de los riesgos para la protección de datos asociados a los algoritmos y sistemas de IA en los que haya tratamientos de datos, garantizando que se implementen medidas adecuadas para proteger los derechos de las personas, como la transparencia en la toma de decisiones automatizadas y la minimización de datos. Además, deberá coordinarse y estar en comunicación con otros equipos para asegurar el cumplimiento de la normativa en la fase de diseño (Privacy by design, PbD) y durante el ciclo de vida de los sistemas. Esto también implica mantenerse actualizado respecto a los avances normativos que tengan que ver con la protección de datos.

7 MECANISMOS DE INDEPENDENCIA

Desde la introducción del Reglamento General de Protección de Datos (RGPD), la figura del Delegado de Protección de Datos (DPO) ha evolucionado dentro de las organizaciones, consolidándose como una pieza clave para garantizar el cumplimiento normativo en materia de protección de datos personales por parte de las organizaciones. Sin embargo, uno de los principios más debatidos y menos comprendidos de este rol es su independencia. Este capítulo profundiza en la necesidad de dicha independencia y en los mecanismos que pueden asegurarla, no solo como un cumplimiento formal del RGPD y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), sino como una base esencial para que el DPO pueda desempeñar su labor de manera efectiva.

> ***"La independencia no es un mero formalismo legal o una casilla más a marcar en el cumplimiento normativo; es un requisito estructural y funcional que garantiza al DPO desempeñar sus responsabilidades sin interferencias."***

Este principio se encuentra en los artículos 37, 38 y 39 del RGPD, que delinean el marco de actuación del DPO, protegiéndolo de conflictos de intereses e influencias indebidas.

Sin embargo, aunque el concepto de independencia pueda parecer sencillo en su definición, en la práctica plantea una serie de desafíos que van más allá de la mera interpretación normativa.

El contexto legal: normativa y jurisprudencia reciente

El RGPD define claramente la figura del DPO en la organización, asignándole una posición clave para garantizar su cumplimiento normativo:

- El artículo 38.3 estipula que el DPO ***no debe recibir instrucciones respecto a cómo llevar a cabo sus funciones y debe reportar directamente al más alto nivel jerárquico.***

- El artículo 38.6 permite que el DPO ***desempeñe otras funciones dentro de la organización, pero a condición de que no den lugar a conflictos de interés.***

En este ámbito, han sido decisivas dos sentencias recientes del ***Tribunal de Justicia de la Unión Europea (TJUE), la del 22 de junio de 2022 en el caso Leistritz AG vs LH (C-534/20)[9] y la del 9 de febrero de 2023 en el caso X-FAB Dresden GmbH & Co. KG vs FC (C-453/21)[10].***

[9] *TJUE de 22 de junio de 2022 en el caso Leistritz AG vs LH (C-534/20)*

[10] *TJUE de 9 de febrero de 2023 en el caso X-FAB Dresden GmbH & Co. KG vs FC (C-453/21)*

En ambas, el TJUE se pronunció sobre la interpretación del artículo 38.3 del RGPD, que considera "aplicable tanto al DPO que forma parte de la plantilla del responsable o del encargado del tratamiento, como a quien desempeña sus funciones en el marco de un contrato de servicio". Se confirmó que los Estados miembros pueden adoptar normativas más estrictas para proteger la posición del DPO, siempre que no interfieran con los objetivos del RGPD. El tribunal también subrayó que la independencia del DPO no es un mero formalismo: su destitución sin causa grave, aunque no esté directamente relacionada con el desempeño de sus funciones, puede ser contraria al RGPD si pone en peligro su independencia funcional.

En España, el artículo 36.2 de la LOPDGDD refuerza esta independencia al señalar que el DPO, cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, "no podrá ser removido ni sancionado" por el desempeño de 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". Esta protección está diseñada para que el DPO pueda actuar con imparcialidad y con plena autonomía.

¿Para qué se requiere la independencia del DPO?

A menudo, la independencia del DPO se considera un atributo secundario, subordinado a las funciones operativas de la organización. Sin embargo, esta percepción es profundamente errónea.

> ***"La independencia no es un fin en sí mismo, sino un medio indispensable para garantizar que el DPO pueda cumplir con las funciones que le asigna el RGPD de manera efectiva y sin interferencias."***

Esta "independencia debe necesariamente permitirles a los DPO ejercer estas funciones de conformidad con el objetivo del RGPD, que tiene como finalidad, en particular, garantizar un nivel elevado de protección de las personas físicas dentro de la Unión" (TJUE, C-534/20). Para ello, el DPO debe auditar, asesorar y garantizar que el tratamiento de los datos personales se realice conforme a los principios de transparencia, proporcionalidad y seguridad. Esto implica que el DPO asuma un papel de control que, en muchos casos, puede actuar como "freno" a prácticas empresariales que, sin la adecuada supervisión, podrían vulnerar los derechos de los interesados.

Este rol de supervisión puede generar tensiones con los objetivos comerciales o estratégicos de la organización, especialmente en áreas de la primera línea de defensa, como TI, Marketing, Finanzas o incluso el departamento jurídico. Si el DPO no dispone de suficiente independencia, estas tensiones podrían traducirse en presiones directas o indirectas que comprometan su capacidad para actuar de manera objetiva y asesoras y supervisar la normativa de protección de datos conforme a lo exigido en el RGPD.

7.1. Interferencias en el desempeño de funciones

Otro obstáculo significativo para la independencia del DPO es la interferencia directa de la dirección. Aunque el Artículo 38.3 RGPD prohíbe que los DPO reciban instrucciones sobre cómo desempeñar sus funciones, la encuesta realizada en 2023 por el Supervisor Europeo de Protección de Datos (EDPS, por sus siglas en inglés), Results of the Survey on the designation and position of the data protection officer in the EU institutions, bodies, offices and agencies , reveló que, en muchos casos, los DPO informaron haber recibido directrices sobre cómo interpretar o aplicar el RGPD, comprometiendo así su capacidad para actuar de manera independiente.

Estas interferencias, sutiles o explícitas, socavan el papel del DPO como garante de la legalidad y protector de los derechos fundamentales de los interesados. Para que el DPO pueda cumplir eficazmente con sus obligaciones, debe poder actuar sin presiones indebidas y con la seguridad de que sus recomendaciones serán valoradas y respectadas.

7.2. Desafíos Prácticos en la Independencia del DPO

A pesar de la claridad de las disposiciones del RGPD y la LOPDGDD, en la práctica, garantizar la independencia del DPO puede ser un desafío significativo, especialmente en empresas privadas donde las presiones comerciales son intensas. Algunos de los problemas clave que afectan la independencia del DPO incluyen:.

7.2.1. El rol del DPO en la protección de la sostenibilidad corporativa

Uno de los mayores retos para garantizar la independencia del DPO es la resistencia cultural dentro de las organizaciones. Muchas empresas, especialmente en sectores donde los datos personales son una materia prima esencial (como marketing, tecnología o finanzas), tienden a percibir el rol del DPO y la protección de datos personales como una función “técnica” o “legal”, una regulación secundaria, desconectada de los objetivos comerciales o, en cualquier caso, subordinada a las necesidades operativas. Esta visión, además de equivocada, compromete tanto el cumplimiento normativo de la organización como su confianza y legitimidad en el mercado actual.

> ***“Lejos de ser un obstáculo para los intereses empresariales, el DPO es un “activo estratégico” que ayuda a la empresa a mitigar riesgos regulatorios, financieros y reputacionales.”***

En un entorno cada vez más regulado y con consumidores conscientes de sus derechos, el papel del DPO no es bloquear el negocio, sino “guiarlo” y asesorarlo para que las operaciones de la empresa se realicen dentro de los márgenes legales, protegiendo los derechos de los interesados y evitando sanciones y pérdidas reputacionales que podrían ser devastadoras. Esto, a su vez, fortalece la confianza de los clientes y socios comerciales.

Para cambiar esta percepción, la alta dirección debe enviar una señal clara de que el cumplimiento de las normativas de protección de datos no es una carga, sino una oportunidad para diferenciarse y ganar la confianza de los consumidores. Los líderes empresariales deben ser los primeros en comprender y apoyar la independencia del DPO, integrándolo en la estrategia global de la empresa y garantizando que sus recomendaciones se consideren en decisiones clave.

La creación de una cultura de cumplimiento requiere formación continua, la difusión de buenas prácticas y una comunicación transparente entre el DPO y las distintas áreas de la empresa. Esta cultura debe reforzar el concepto de que la privacidad es un valor empresarial, y que el DPO es un actor fundamental en la protección de este valor.

Un DPO independiente puede proporcionar una visión objetiva de los riesgos que enfrenta la organización, algo fundamental para la toma de decisiones estratégicas. Por ejemplo, el DPO puede anticiparse a problemas que, de otro modo, podrían resultar en brechas de datos o sanciones, asegurando que la empresa mantenga su integridad y reputación. De este modo, el DPO se convierte en un protector no solo de los derechos individuales, sino también de la sostenibilidad a largo plazo de la empresa.

Para que esta función pueda ejercerse de manera efectiva, la organización debe reconocer que el DPO no puede ser tratado como cualquier otro miembro del equipo, subordinado a los intereses de una dirección o área específica. Su independencia es crucial para que pueda actuar como un contrapeso efectivo dentro de la estructura de gobierno corporativo, velando por el cumplimiento de las normativas de protección de datos en un contexto donde los incentivos comerciales o de eficiencia operativa podrían, de otro modo, prevalecer.

7.2.2. Reporte y dependencia jerárquica del DPO

Para garantizar su independencia, el RGPD establece que el DPO debe reportar directamente al más alto nivel jerárquico de la organización. En la práctica, muchas organizaciones todavía cometen el error de asignar al DPO a áreas operativas o de negocio, a la "primera línea de defensa", como el departamento de TI, Marketing, Finanzas que se ven tentadas a tratar los datos personales como un "activo comercial" más. Para estas áreas, los datos son esenciales para optimizar procesos, segmentar clientes o crear nuevas oportunidades de negocio. Es precisamente en este contexto donde el DPO debe ejercer su función de asesoramiento y supervisión para que la organización pueda garantizar que el uso de los datos se ajuste a los principios de transparencia, minimización y proporcionalidad que establece el RGPD.

Sin embargo, cuando el DPO depende jerárquicamente de estas áreas, su capacidad para actuar con independencia podría verse severamente limitada. Los objetivos de algunas primeras línea de defensa – como maximizar la eficiencia y los beneficios – pueden entrar en conflicto directo con los principios de protección de datos. Áreas como TI o Marketing podrían tener incentivos para explotar al máximo los datos disponibles, aunque esto implique prácticas cuestionables en cuanto a privacidad, como la recolección masiva de datos sin una base legal adecuada o el tratamiento de datos personales sin el consentimiento informado de los interesados.

La dependencia jerárquica del DPO de la primera línea de defensa no solo es un riesgo teórico, sino una realidad cotidiana en muchas organizaciones. Un ejemplo común es la gestión de incidentes de seguridad que involucran datos personales. Imaginemos un escenario donde una organización sufre un incidente que expone datos personales de clientes. El CIO y el equipo de TI podrían verse tentados a minimizar el incidente para evitar repercusiones regulatorias o mediáticas. En este tipo de situaciones, el RGPD exige la notificación tanto a la autoridad de control como a los afectados, pero si el DPO depende del CIO, su capacidad para cumplir con esta obligación de manera objetiva puede verse comprometida. El CIO, preocupado por las sanciones o el daño a la reputación de la empresa, puede presionar al DPO para evitar notificar el incidente, lo que no solo constituye una violación del RGPD, sino que pone en riesgo la sostenibilidad a largo plazo de la organización.

Estas situaciones no son infrecuentes, y evidencian la necesidad de que el DPO esté alineado con una línea de defensa diferente, que no esté involucrada directamente en la toma de decisiones operativas sobre el tratamiento de datos. La independencia del DPO va más allá de la cuestión formal de "quién firma su contrato"; se trata de garantizar que no esté subordinado a áreas cuyos intereses puedan entrar en conflicto con los principios de protección de datos.

Una buena práctica en este sentido, para que el DPO pueda desempeñar su función de manera efectiva, es su alineación con la "segunda línea de defensa", donde se ubican otras funciones de control, como Cumplimiento y Riesgos, que comparten el objetivo de supervisar y garantizar el cumplimiento normativo, sin intervenir directamente en decisiones operativas que puedan comprometer su objetividad e independencia.

Asimismo, resulta recomendable la creación de Comités de Privacidad, en los que el DPO tenga un papel destacado y se puedan debatir y resolver posibles conflictos de interés. Estos comités, integrados por miembros de diferentes áreas, garantizan que las decisiones sobre el tratamiento de datos se tomen de manera colegiada y transparente, evitando que el DPO se vea aislado o presionado por intereses comerciales específicos.

No obstante, la experiencia acumulada en estos años demuestra que, en determinadas organizaciones de gran complejidad y estructura, la ubicación del DPO en la primera línea de defensa también ha podido resultar efectiva. Esto ha sido posible gracias a la implementación de sinergias organizativas que han permitido mantener la independencia funcional del DPO, conforme a lo establecido en el RGPD. Por tanto, la determinación de la existencia de conflictos de interés en estos casos debe efectuarse de forma individualizada, considerando el conjunto de circunstancias pertinentes, la estructura organizativa del responsable o encargado del tratamiento y la normativa aplicable, incluidas las políticas internas de la organización (TJUE, C-453/21, apartado 45).

Aunque persistan los desafíos en la definición de la **ubicación idónea** para el DPO, cada organización debe evaluar su propio modelo de gobernanza, asegurándose de que el DPO pueda desempeñar sus funciones con plena autonomía e independencia. Como ya señalamos en la introducción de esta segunda edición del Libro Blanco del DPO, en los años transcurridos hemos aprendido mucho sobre los distintos modelos organizativos del DPO: desde su ubicación en estructuras internas hasta su externalización o la configuración de equipos colegiados, en los que cada organización ha ido encontrando su propio camino para garantizar la eficacia e independencia de esta función.

Lo crucial es que, al final del día, el DPO pueda constatar que mantiene los rasgos esenciales de dicha independencia, que detallamos en este capítulo.

7.2.3. El conflicto de intereses: un reto constante

El conflicto de intereses es uno de los riesgos más serios que enfrenta la independencia del DPO. Como establece el artículo 38.6 del RGPD, el DPO puede desempeñar otras funciones dentro de la organización, siempre y cuando estas no den lugar a conflictos de intereses. Sin embargo, en la práctica, identificar y gestionar estos conflictos puede ser complejo, ya que los roles y responsabilidades dentro de las organizaciones tienden a superponerse.

Un caso claro de incompatibilidad surge cuando el DPO asume responsabilidades en el área de Legal, donde su rol de supervisor independiente en protección de datos puede verse en conflicto con las funciones de defensa o asesoría jurídica. Este conflicto de interés fue señalado en la reciente resolución de la AEPD (EXPEXP202211394, 2024iii), que subraya que el DPO no debe representar a la organización en procedimientos sancionadores ni presentar alegaciones en su defensa, ya que *"implica una defensa activa y una declaración de posición"*. La AEPD considera que existe *"conflicto de intereses, pues el DPO no puede simultáneamente informar y asesorar al responsable del tratamiento y, al mismo tiempo, actuar en su defensa. Esta dualidad de roles en la misma persona, el DPO; compromete de manera grave su independencia y objetividad, pilares fundamentales para el adecuado ejercicio de sus funciones conforme a la normativa vigente."*

De forma similar, los conflictos de interés pueden surgir cuando el DPO asume funciones adicionales en TI o en Operaciones, áreas donde puede sentirse presionado a priorizar la eficiencia operativa sobre la protección de los derechos de los interesados, lo que comprometería su independencia.

Con la reciente publicación del Reglamento de IA de la Unión Europea (AI Act), se abre un nuevo espacio para debatir la posibilidad de conflicto para el DPO en la gestión de la IA. Será crucial diferenciar entre la gobernanza normativa de la IA y su explotación operativa dentro de las organizaciones. Aunque algunos sectores de la doctrina anticipan posibles conflictos de interés, el AI Act, enfocado en la gestión de riesgos y cumplimiento normativo de la IA, no debería generar una tensión directa con la función actual del DPO. En cambio, otros roles, como el Chief Data Officer (CDO), se centran en maximizar el valor de la IA para el negocio. A medida que surgen nuevas figuras, como las Oficinas Técnicas de IA, el DPO podría desempeñar un papel fundamental en la supervisión normativa sin comprometer su independencia.

Por ello, las autoridades de control recomiendan una separación estructural entre el DPO y todas estas funciones. En organizaciones donde dicha separación sea difícil, se recomienda implementar medidas como la clara definición de responsabilidades, el establecimiento de canales de reporte independientes hacia la alta dirección y auditorías internas periódicas para gestionar posibles conflictos de interés.

"La determinación de la existencia de un conflicto de intereses, en el sentido del artículo 38.6 del RGPD, "debe efectuarse caso por caso, sobre la base de una apreciación del conjunto de las circunstancias pertinentes, en particular, de la estructura organizativa del responsable del tratamiento o de su encargado y a la luz de toda la normativa aplicable, incluidas las eventuales políticas de estos últimos" (TJUE, C-453/21, apartado 45)."

7.2.4. Recursos y formación

El acceso a recursos suficientes es otro aspecto clave para garantizar la independencia del DPO. El RGPD establece que los DPO deben contar con los recursos necesarios para llevar a cabo sus tareas, lo que incluye personal, infraestructura y acceso a formación continua. Sin embargo, en muchas organizaciones, los DPO se quejan de que no disponen de presupuesto propio o del apoyo técnico y humano necesario para realizar su labor de manera efectiva.

Esta falta de recursos no solo compromete la independencia del DPO, sino que también reduce su capacidad para implementar las medidas necesarias para asegurar el cumplimiento normativo. Esto es especialmente crítico en organizaciones grandes o aquellas con actividades de tratamiento de datos complejas, donde el volumen de datos y la complejidad de los procesos requieren una supervisión rigurosa.

No obstante, esta responsabilidad no recae únicamente en las organizaciones. Los DPO también deben aprovechar activamente los recursos que se les asignan, especialmente en lo que respecta a su formación. Es importante que los DPO mantengan un enfoque proactivo hacia su desarrollo profesional, buscando certificaciones que acrediten sus conocimientos, como el Certificado de Delegado de Protección de Datos de la AEPD, para reforzar su cualificación y credibilidad.

7.2.5. Falta de integración en procesos críticos

A menudo, los DPO no son incluidos en decisiones clave que implican el tratamiento de datos personales, lo que limita su capacidad para prevenir riesgos. La falta de participación del DPO en procesos como las evaluaciones de impacto sobre la protección de datos (DPIA) o en la gestión de incidentes de seguridad es un problema recurrente. Según el RGPD, el DPO debe ser consultado de manera oportuna y adecuada en todos los asuntos que afecten el tratamiento de datos personales, pero en la práctica, esta consulta es a menudo insuficiente o inexistente.

7.3. Mecanismos para garantizar la independencia de DPO

La independencia del DPO no puede garantizarse únicamente mediante la estructura jerárquica; requiere un enfoque proactivo por parte de las organizaciones. Estas deben implementar mecanismos que refuercen esta independencia y que protejan al DPO de posibles presiones o influencias indebidas.

A continuación, se detallan algunos de los mecanismos clave que deben considerarse:

7.3.1. Reportar al más alto nivel de la organización

El DPO debe reportar directamente al más alto nivel de gestión, a la alta dirección o al consejo de administración, sin intermediarios. Esto garantiza que su labor sea visible y tenga el respaldo necesario para actuar con independencia.

Este mecanismo asegura que las recomendaciones del DPO sean escuchadas y que tenga la influencia necesaria para impactar en las decisiones estratégicas de la empresa. Además, el reporte directo al consejo de administración o a la alta dirección evita que el DPO quede subordinado a intereses de áreas operativas específicas que podrían entrar en conflicto con la protección de datos.

7.3.2. Separación de funciones

El DPO no debe tener responsabilidades que impliquen la toma de decisiones sobre el tratamiento de datos personales. Para evitar conflictos de interés, es esencial que las funciones del DPO no se solapen con otras responsabilidades operativas dentro de la empresa. Las políticas internas deben identificar claramente los roles incompatibles con las responsabilidades del DPO, asegurando que este no esté involucrado en la toma de decisiones sobre el tratamiento de datos personales.

El RGPD permite que el DPO desempeñe otras funciones, pero estas no deben comprometer su independencia. Esto significa que las organizaciones deben asegurarse de que el DPO no ocupe roles en departamentos donde las presiones para maximizar el uso de datos personales pueden entrar en conflicto con los principios de minimización y legalidad del tratamiento.

7.3.3. Recursos suficientes y autonomía presupuestaria

El acceso a los recursos adecuados es una condición sine qua non para la independencia del DPO. La falta de personal, infraestructura o acceso a formación continua limita la capacidad del DPO para cumplir con sus responsabilidades de manera independiente. En este sentido, las empresas deben asegurar que el DPO cuente con un presupuesto propio que le permita acceder a las herramientas esenciales, como software de

auditoría, formación especializada y la contratación de servicios externos para llevar a cabo auditorías o recibir asesoramiento en áreas clave de protección de datos. Esta autonomía presupuestaria es clave para que el DPO no dependa exclusivamente de otras áreas de la empresa que puedan tener intereses distintos en el uso de datos personales.

Además, los incentivos para el DPO deben estar claramente orientados a la protección de datos y al cumplimiento normativo, evitando que se prioricen intereses económicos o comerciales, incluso de forma indirecta, mediante la satisfacción de objetivos, o los también denominados "clientes", internos. Entre los objetivos recomendables figuran la efectividad en la gestión de incidentes de brechas de datos, la implementación de medidas preventivas y la calidad de la formación sobre privacidad a los empleados. Para asegurar que los incentivos no comprometan su independencia, es recomendable que un comité de auditoría o de privacidad supervise su asignación, garantizando que estén alineados exclusivamente con la misión de protección de datos.

7.3.4. Participación activa en procesos de decisión

El DPO debe ser consultado de manera proactiva en todas las decisiones relevantes que afecten al tratamiento de datos personales. Esto incluye la realización de evaluaciones de impacto (DPIA), la gestión de incidentes de seguridad y brechas de datos personales y la planificación de nuevos proyectos tecnológicos que involucren el procesamiento de datos a gran escala o el uso de tecnología que está ya teniendo un claro impacto sobre los datos personales, sin tener que esperar al futuro, como la irrupción de la Inteligencia Artificial, que con la entrada en vigor de la LIA de la UE (la "AI Act") en 2024, activa el debate del papel que tiene que desempeñar el DPO al respecto. Integrar al DPO en estos procesos desde el inicio no solo garantiza que se cumplan los requisitos del RGPD, sino que también permite que la empresa identifique y mitigue los riesgos a tiempo, evitando sanciones o daños a su reputación.

7.3.5. Políticas y transparencia

Las organizaciones deben documentar de manera clara las funciones y responsabilidades del DPO, así como los procedimientos para evitar conflictos de intereses. Esta documentación debe revisarse periódicamente para asegurar que el DPO pueda actuar con la autonomía que exige el RGPD.

Las organizaciones deben establecer procedimientos claros para que el DPO presente informes periódicos sobre el estado del cumplimiento y las áreas de riesgo, fomentando su transparencia. Esto refuerza la visibilidad del DPO dentro de la organización y asegura que su trabajo esté alineado con los objetivos corporativos, pero sin comprometer su independencia.

7.3.6. Comités de Privacidad

La creación de comités específicos de privacidad o grupos de trabajo multidisciplinarios (como las oficinas técnicas de gobernanza de la IA), pueden ser una herramienta eficaz para reforzar la independencia del DPO. Estos comités pueden actuar como un foro donde se discutan y resuelvan posibles conflictos de interés, además de apoyar al DPO en la toma de decisiones estratégicas relacionadas con la protección de datos.

Estos comités también permiten que la alta dirección esté informada sobre las preocupaciones del DPO y facilite una toma de decisiones colegiada, evitando que los intereses comerciales de departamentos específicos prevalezcan sobre las obligaciones legales.

7.3.7. Auditorías independientes

Realizar auditorías externas sobre el funcionamiento del DPO y su grado de independencia puede ayudar a identificar posibles debilidades en la estructura organizativa y a proponer soluciones para mejorar la autonomía del DPO.

7.3.8. Protección frente a despidos injustificados

Y, por último, la independencia del DPO no puede ser efectiva si no está protegida frente a sanciones o despidos injustificados por el desempeño de sus funciones. El Artículo 38.3 RGPD, establece que el DPO no puede ser destituido ni sancionado por cumplir con sus obligaciones. Sin embargo, en la práctica, algunos DPOs han reportado presiones para relajar su supervisión o minimizar los riesgos, especialmente cuando estos conflictos afectan directamente a los intereses comerciales de la empresa.

Para asegurar una independencia real, las organizaciones deben crear un entorno donde el DPO pueda actuar sin miedo a represalias, y donde su función de supervisión sea valorada y respaldada por la alta dirección. Esta protección también debe estar formalizada en políticas internas, que definan claramente las responsabilidades y los derechos del DPO y establezcan un mecanismo de revisión interna en caso de disputas sobre su desempeño.

En su sentencia de 22 de junio de 2022, Leistritz (C 534/20, EU:C:2022:495, apartados 20 y 21), el TJUE, tras declarar que el RGPD no define los conceptos «destituido», «sancionado» y «por desempeñar sus funciones», que figuran en ese artículo 38, apartado 3, segunda frase, subrayó, en primer término, que, "conforme a su sentido habitual en el lenguaje corriente, la prohibición impuesta al responsable o encargado del tratamiento de destituir a un delegado de protección de datos o de sancionarlo significa que dicho delegado debe estar protegido contra cualquier decisión que ponga fin a sus funciones, le sea desfavorable o constituya una sanción". "Pues bien, puede constituir tal decisión una medida de destitución de un delegado de protección de datos adoptada por su empleador y que tendría como consecuencia relevar al delegado de sus funciones en el seno

del responsable del tratamiento o de su encargado". (Stc TJUE de 9 de febrero de 2023, en el caso X-FAB Dresden GmbH & Co. KG vs FC (C-453/21), apartados 21 y 22).

El artículo 38, apartado 3, segunda frase, del RGPD, "al amparar al delegado de protección de datos contra cualquier decisión que ponga fin a sus funciones, le sea desfavorable o constituya una sanción, cuando tal decisión esté relacionada con el desempeño de sus funciones, debe considerarse dirigido esencialmente a preservar la independencia funcional del delegado de protección de datos y, por lo tanto, a garantizar la efectividad de las disposiciones del RGPD" (sentencia de 22 de junio de 2022, Leistritz, C 534/20, EU:C:2022:495, apartado 28).

7.4. Independencia del DPO y Resoluciones de las Autoridades de Control de Protección de Datos

La independencia del DPO es un elemento crucial para garantizar el cumplimiento normativo en materia de protección de datos. No obstante, garantizar esta independencia no es tarea fácil, ya que requiere un cambio cultural dentro de las organizaciones, donde las áreas operativas comprendan que el papel del DPO no es un freno, sino una garantía para la sostenibilidad y legitimidad de la empresa a largo plazo. Y, como antes referenciamos del TJUE, habrá que estar a "caso por caso, sobre la base de una apreciación del conjunto de las circunstancias pertinentes, en particular, de la estructura organizativa del responsable del tratamiento o de su encargado y a la luz de toda la normativa aplicable, incluidas las eventuales políticas de estos últimos".

Los desafíos para la independencia del DPO, como los conflictos de interés, la falta de recursos o las interferencias de la alta dirección, deben abordarse con mecanismos claros que refuercen su autonomía.

Las organizaciones que no tomen en serio la independencia del DPO corren el riesgo de comprometer tanto su cumplimiento normativo como su reputación. En un entorno donde los derechos de privacidad son cada vez más valorados, contar con un DPO independiente no solo es una obligación legal, sino una ventaja competitiva que puede marcar la diferencia entre una empresa que prospera en el largo plazo y una que se enfrenta a sanciones y pérdida de confianza por parte de sus clientes.

Esta independencia no quiere decir que el DPO no pueda ser objeto de control e incluso ser destituido de su puesto, sino que como clarifica el TJUE en las sentencias que reiteradamente hemos referido en todo este capítulo, "la protección reforzada del DPO no ha de poner en peligro la consecución de los objetivos del RGPD". Pues bien, "así sucedería si esta impidiera cualquier destitución, por parte de un responsable o de un encargado del tratamiento, de un delegado de protección de datos que ya no tuviera las cualidades profesionales requeridas para ejercer sus funciones", de conformidad con el artículo 37, apartado 5, del RGPD, o "que no las cumpliera conforme a las disposiciones de ese Reglamento" (véase, en este sentido, la sentencia de 22 de junio de 2022, Leistritz, C 534/20, EU:C:2022:495, apartado 35).

Es fundamental que las empresas implementen los mecanismos necesarios para asegurar que el DPO pueda desempeñar su función sin interferencias, con pleno acceso a la alta dirección y con el respaldo necesario para actuar con objetividad.

"La independencia del DPO es, en última instancia, una garantía para la organización misma, protegiéndola de los riesgos asociados a un uso inadecuado de los datos personales y asegurando que sus prácticas sean acordes con los principios éticos y legales que rigen el tratamiento de datos en la actualidad."

7.4.1. Regulación del DPO en el RGPD y LOPDGDD

El R**eglamento General de Protección de Datos (RGPD)** establece en sus artículos **37, 38 y 39** las obligaciones relativas al **Delegado de Protección de Datos (DPO**), regulando su designación, posición en la organización, funciones y recursos. Su incumplimiento puede constituir una infracción sancionable conforme a los artículos **83.4 y 83.2 del RGPD.**

En el ordenamiento español, la **Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) c**omplementa el RGPD y regula aspectos específicos del DPO, estableciendo además un régimen sancionador nacional.

7.4.2. Infracciones Relacionadas con el DPO en el RGPD y LOPDGDD

RGPD:

- **Artículo 37. Designación del Delegado de Protección de Datos:** La falta de designación de un DPO cuando sea obligatoria constituye una infracción grave. El RGPD establece criterios específicos para determinar cuándo es preceptiva dicha designación, tanto en el sector público como en el privado.

- **Artículo 38. Posición del Delegado de Protección de Datos:** Se consideran infracciones situaciones que comprometan la **independencia del DPO,** como la falta de apoyo en el desempeño de sus funciones, la ausencia de recursos adecuados o la imposición de instrucciones que puedan influir en sus decisiones.

- **Artículo 39. Funciones del Delegado de Protección de Datos:** El incumplimiento de las funciones asignadas al DPO, incluyendo la supervisión del cumplimiento normativo, la formación del personal y la cooperación con la autoridad de control, también constituye una infracción.

LOPDGDD:

- **Artículo 34. Designación de un Delegado de Protección de Datos:** Refuerza la obligación de designar un DPO en determinados supuestos específicos en España, ampliando los criterios del RGPD, por ejemplo, para colegios profesionales, operadores de juego online, o entidades que traten grandes volúmenes de datos sensibles.

- **Artículo 65 – Infracciones:** Las infracciones relacionadas con el DPO se tipifican como **leves, graves o muy graves.** La falta de designación obligatoria de un DPO, la ausencia de colaboración con la autoridad de control o la falta de comunicación de su nombramiento se consideran infracciones **graves** o incluso **muy graves**, dependiendo de las circunstancias del caso.

7.4.3. Régimen Sancionador en el RGPD y LOPDGDD

RGPD:

- **Artículo 83.4, letra a):** Las infracciones de los artículos 37, 38 y 39 pueden dar lugar a multas administrativas de hasta **10 millones de euros** o, en el caso de una empresa, hasta el **2 % del volumen de negocio total anual** global del ejercicio financiero anterior, optándose por la cantidad de mayor cuantía.

- **Artículo 38.2:** Establece los **criterios para la determinación de la cuantía de la sanción,** incluyendo la naturaleza, gravedad y duración de la infracción, el carácter doloso o negligente, las medidas adoptadas para mitigar el daño, y el grado de cooperación con la autoridad de control.

- **Artículo 58.2:** Además de las sanciones económicas, las autoridades de control pueden imponer medidas correctivas, como **advertencias, apercibimientos o la orden de subsanar el incumplimiento.**

LOPDGDD:

- **Artículo 71 – Tipificación de las infracciones:** Las infracciones se clasifican en tres niveles:

  - **Muy graves:** Multas de hasta **20 millones de euros o el 4 % del volumen de negocio anual global** (cuando corresponda, de acuerdo con el RGPD).
  - **Graves:** Multas de hasta **10 millones de euros o el 2 % del volumen de negocio anual global.**
  - **Leves:** Sanciones económicas menores, o bien apercibimientos, especialmente en el caso de administraciones públicas.

- **Artículo 77 – Régimen aplicable a las Administraciones Públicas:** · Artículo 77 – Régimen aplicable a las Administraciones Públicas: En el caso de las administraciones públicas, la LOPDGDD establece la posibilidad de aplicar sanciones no económicas, como apercibimientos o la adopción de medidas correctivas, dado que no se imponen **sanciones económicas** a las entidades públicas en la mayoría de los casos.

7.4.4. Resoluciones de las Autoridades de Control

La inclusión de estas resoluciones en el análisis permite comprender mejor los **límites y obligaciones** establecidos por el RGPD y la LOPDGDD, así como las **consecuencias jurídicas** derivadas de su incumplimiento.

"Las resoluciones dictadas por las autoridades de control, aunque aún limitadas en número, evidencian una tendencia creciente a proteger la figura del DPO y sancionar prácticas que comprometan la independencia, los recursos y la ausencia de conflictos de interés en el ejercicio de su función."

7.4.4.1 Resoluciones de la AEPD

Si bien la AEPD no ha sido especialmente activa en la imposición de sanciones por incumplimientos de los artículos **37, 38 y 39 del RGPD**, existen algunas resoluciones significativas que abordan aspectos clave relacionados con la independencia y las funciones del DPO:

- **Falta de designación preceptiva de DPO:** la AEPD ha impuesto con frecuencia sanciones de apercibimiento a un número elevado de administraciones públicas. En cuanto a sanciones a entidades privadas por este motivo, destaca el PS/140/2022[11], en el que se sanciona a cadena de restaurantes de comida rápida con 20.000 euros por no haber designado a un DPD cuando, bajo el criterio de la agencia, dicha cadena de restaurantes trataba datos personales que, debido a su naturaleza, alcance y/o fines, requerían una observación habitual y sistemática de interesados a gran escala. Aunque la sancionada alegó que su actividad no implicaba la designación obligatoria de un DPD, la AEPD consideró que las actividades de marketing llevadas a cabo por la cadena a gran escala son indisociables de su actividad principal, por lo que si era preceptiva la designación de un DPD.

- **Conflictos de interés:** en relación a la incompatibilidad de funciones y conflictos de interés, no existen por parte de la AEPD un gran número de resoluciones sancionadoras que aborden dicha cuestión. Destaca la resolución del recurso de reposición presentado por la Secretaría de Estado de Seguridad contra el PS/382/2023[12], en el que la AEPD indica que la presentación de alegaciones en el marco de un procedimiento sancionador por parte del DPD representa un conflicto de intereses y compromete su independencia, ya que implica una defensa activa en procedimientos sancionadores, lo cual es incompatible con su función de asesoramiento interno. En este caso, la AEPD argumentó que el responsable del tratamiento también tiene la capacidad para gestionar las comunicaciones con la AEPD y no puede delegar funciones administrativas que pongan en riesgo la imparcialidad del DPD. La Agencia concluyó que la actuación del DPD conlleva una infracción sustantiva debido a la falta de independencia y objetividad, ya que el DPD no puede simultáneamente asesorar y defender al responsable del tratamiento, ya que esto compromete su independencia y objetividad.

[11] *Procedimiento Nº: PS/00140/2022.*

[12] *Resolución de Recurso de Reposición*

7.4.4.2 Resoluciones de otras autoridades de control europeas

BÉLGICA. En 2020, la Autoridad de Protección de Datos belga [Autorité de protection des données - APD / Gegevensbeschermingsautoriteit - GBA[13], impuso una multa de **50.000 euros** a una compañía fundamentada el incumplimiento del art. 38.6 del RGPD, principalmente, porque el DPD asumía, al mismo tiempo, roles de superior jerárquico o jefe de otros departamentos dentro de la entidad (i cumplimiento, gestión de riesgos y auditoría interna), roles estos que le otorgan poder de decisión sobre los fines y los medios del tratamiento dentro del departamento en cuestión. En este sentido, el hecho de que el DPD tenga poder de decisión sobre determinados tratamientos impide que pueda ejercer sus funciones de supervisión en materia de protección de datos de forma independiente respecto de dichos tratamientos, derivándose en consecuencia el conflicto de intereses que la norma sanciona, a pesar de los argumentos expuestos por la empresa respecto de la supuesta función meramente consultiva de las posiciones ostentadas en los distintos departamentos. La autoridad Belga concluyó que no puede sostenerse la exigida independencia en la persona que no sólo forma parte de un determinado departamento, sino que es responsable de asesorarle y, al mismo tiempo, ejerce la función de DPD, máxime cuando no se prueba la existencia de medidas encaminadas a impedir el conflicto de intereses que se pretende evitar. También esta misma autoridad, determinó en 2021[14] la existencia de un conflicto de interés cuando una persona ocupa simultáneamente el rol de DPO y jefe de los departamentos de Gestión de Riesgos Operacionales.

CROACIA. En septiembre de 2023, la Agencia de Protección de Datos Personales croata [Agencija za zaštitu osobnih podataka – AZOP], sancionó con **15.000 euros**[15] a un grupo hotelero por haber designado como DPO al **director del propio hotel**, situación que generaba un conflicto de interés inherente debido a la **incompatibilidad entre la gestión operativa** y las funciones de supervisión propias del DPO. En este caso, el director del hotel y el DPD eran responsables tanto de tomar decisiones de gestión sobre el tratamiento de datos como de garantizar el cumplimiento de dichas actividades de tratamiento, lo que es claramente incompatible. (artículo 38.6 del RGPD).

ITALIA. En abril de 2024[16], el **Garante per la Protezione dei Dati Personali** se ha pronunciado recientemente en relación a las incompatibilidades del DPD con otros roles, imponiendo una sanción a un ente público por designar un DPD que a su vez ocupaba otras funciones profesionales, como el de jefe de varios servicios dentro del Organismo (Secretaría del Director del Sector I, Asistencia a los Organismos, Sistemas de Información, Turismo y, en última instancia, el Servicio Jurídico). En este caso el Garante concluye que DPD designado, al ocupar varios cargos, carecía de los recursos necesarios, en particular del tiempo, y se encontraba potencialmente en una situación de conflicto de intereses, lo que contravenía el artículo 38.2 y el artículo 38.6 del RGPD.

[13] *APD/GBA (Belgium) - 18/2020*

[14] *APD/GBA (Belgium) - 141/2021; Dossiernummer : DOS-2020-03763*

[15] *AZOP (Croatia) - Decision 26-09-2023*

[16] *Garante per la protezione dei dati personali (Italy) - 10013391*

- **LUXEMBURGO:** Destacar[17], la sentencia del alto **Tribunal de Luxemburgo** (equivalente al Tribunal Supremo Español), que aborda el papel del DPD en un grupo de empresas, y que en este caso viene a ratificar una multa de 18.000 € impuesta por la Autoridad de Protección de Datos de Luxemburgo (CNPD) a una empresa por no haber involucrado directamente a su DPD en asuntos de protección de datos y por no haberle proporcionado recursos suficientes. La empresa formaba parte de un grupo que había designado un DPD único para todas sus entidades (según el artículo 37.2 del RGPD) y un abogado local como punto de contacto en Luxemburgo. Se creó un Comité de Protección de Datos en Luxemburgo, pero el DPD no era miembro y solo recibía información a través de actas y preguntas del punto de contacto local. De hecho, el DPO solo intervenía cuando un interesado no estaba satisfecho con la respuesta del punto de contacto local. La empresa tampoco demostró que el DPD fuera consultado previamente sobre la constitución del Comité de Protección de Datos específico en Luxemburgo. La única persona con funciones de protección de datos en Luxemburgo era el abogado de la empresa, lo que limitaba su capacidad para desempeñar correctamente la función de apoyo al DPD ya que, dada la magnitud de la empresa (70 sedes, entre 1600 y 2100 empleados y 25.000 clientes diarios), era necesario contar con al menos un profesional a tiempo completo dedicado a la protección de datos.

También en Luxemburgo, esta DPA[18] consideró que el DPO estaba involucrado en tareas que podrían resultar en un conflicto de intereses al solapar su rol con el de Jefe de Cumplimiento. En este caso, el DPD participaba en la determinación e implementación del tratamiento de datos personales como parte de sus funciones como Jefe de Cumplimiento y, por lo tanto, estaba obligado a evaluar las prácticas de tratamiento de datos que él mismo había implementado. Ninguna de las medidas adoptadas por el responsable del tratamiento para mitigar el riesgo de conflicto de intereses (como el hecho de que, en caso de un posible conflicto de intereses, el tratamiento en cuestión tendría que ser refrendado por el superior jerárquico del DPO) se consideró suficiente.

[17] *TADM - 46401*

[18] *CNPD (Luxemburgo) - Délibération n°37FR/2021 - GDPRhub*

8 EL PERFIL DEL DELEGADO DE PROTECCIÓN DE DATOS

8.1. Marco legal

Una vez nombrado el DPO, el artículo 38, apartado 1, del RGPD y el artículo 44, apartado 1, del RGPD exigen que los responsables y encargados del tratamiento mantengan al RPD «implicado, adecuada y oportunamente, en todas las cuestiones relacionadas con la protección de datos personales»; el artículo 38, apartado 2, del RGPD y el artículo 44, apartado 2, del RGPD obligan a los responsables y encargados del tratamiento a «apoyar» al DPO «facilitándole recursos» para sus tareas, y el artículo 38, apartado 3, del RGPD y el artículo 44, apartado 3, del RGPD exigen que el responsable sea independiente de la influencia de dichos responsables y encargados del tratamiento. Por su parte, el artículo 39 del RGPD y el artículo 45 del RGPD establecen una serie de tareas para el DPO, entre las que se incluye la de supervisar y asesorar sobre el cumplimiento del RGPD y cooperar con las autoridades de control. También se pretende que los DPO sean figuras visibles que puedan interactuar con los interesados; los artículos 13, apartado 1, letra b), 14, apartado 1, letra b), y 37, apartado 7, del RGPD, y los artículos 15, apartado 1, letra b), 16, apartado 1, letra b), y 43, apartado 3, del RGPD exigen que los responsables del tratamiento pongan a disposición los datos de contacto del DPO, de modo que pueda contactárseles en caso necesario.

La legislación de protección de datos de la UE también ofrece soluciones para adaptar el nombramiento y el funcionamiento del RPD a las necesidades específicas del responsable o encargado del tratamiento de que se trate, teniendo en cuenta la complejidad de su tratamiento de datos personales. De conformidad con el artículo 38, apartado 6, del RGPD y el artículo 44, apartado 6, del RGPD, la función puede incluirse como parte de otro puesto (siempre que las demás tareas y obligaciones de la función no den lugar a un conflicto de intereses) y, según el apartado 3 de ambas disposiciones, el DPO «informará directamente al más alto nivel directivo del responsable o del encargado del tratamiento». Además, el artículo 37, apartados 2 y 3, del RGPD, y el artículo 43, apartado 2, del RGPD, permiten que varios responsables o encargados del tratamiento (ya sean empresas u organismos públicos con arreglo al RGPD o instituciones y organismos de la UE con arreglo al RGPD) designen a un único delegado de protección de datos, siempre que todos puedan acceder

fácilmente a él. Entretanto, el artículo 37, apartado 6, del RGPD y el artículo 43, apartado 4, del RGPD establecen que un RPD no tiene que ser necesariamente un miembro de pleno derecho del personal y puede, en cambio, desempeñar sus funciones sobre la base de un contrato de servicios. Cabe destacar que el RGPD no considera estas dos opciones en pie de igualdad, ya que el artículo 43, apartado 4, establece que el RPD será un miembro del personal de la institución de la UE; sólo cuando se tenga en cuenta su tamaño, y si no se ejerce la opción de tener un DPO compartido con otra institución de la UE, una institución de la UE podrá designar a un DPO sobre la base de un contrato de servicios. Cada una de estas disposiciones es especialmente útil para los responsables y encargados del tratamiento más pequeños que deseen emplear a un DPO pero no dispongan de los recursos necesarios para contratar a un miembro del personal dedicado y permanente. Sin embargo, es muy importante que, incluso cuando el DPO tenga otras funciones o trabaje a tiempo parcial, las tareas del DPO sigan siendo las mismas y, como se ha indicado anteriormente, los responsables y encargados del tratamiento deben asegurarse de que proporcionan el tiempo, la formación y los recursos adecuados para que el DPO realice su trabajo correctamente.

El RGPD establece las condiciones en las que debe designarse un DPO, pero los responsables o encargados del tratamiento también pueden optar por designarlo voluntariamente. Como método de cumplimiento, esto puede ser extremadamente útil; tener un experto en protección de datos que esté vinculado a los procesos de planificación y toma de decisiones ayuda no solo con el principio de responsabilidad en virtud del artículo 5, apartado 2, del RGPD, sino también con la obligación del artículo 24, apartado 1, de aplicar medidas técnicas y organizativas apropiadas para garantizar el cumplimiento del RGPD, las obligaciones del artículo 25 hacia la protección de datos desde el diseño y por defecto, entre muchas otras.

8.2. Cualificación

El DPO será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones encomendadas por el propio RGPD, que veremos en el siguiente apartado.

Por su parte, el GT29 señala que el conocimiento especializado se debe determinar en función de las operaciones de tratamiento de datos que se lleven a cabo (sensibilidad, complejidad y el volumen de datos objeto de tratamiento) y de la protección exigida para los datos personales tratados. Debe tratarse de un DPO con un profundo conocimiento del Reglamento, del sector y del negocio de la propia organización (en particular, cuando se sustente en el tratamiento de datos personales) para facilitar la innovación y competitividad a la vez que se asegura del derecho fundamental a la protección de datos.

De esta manera, la Confederation of European Data Protection Organitations (CEDPO) señala que el hecho de tener conocimientos especializados en derecho no debe ser algo exclusivo de licenciados en derecho, sino que dichos conocimientos en materia de protección de datos pueden tenerlos tanto perfiles jurídicos como técnicos.

8.3. Experiencia Profesional

El DPO debe contar con conocimiento y experiencia, acreditada y reconocida en los siguientes campos:

a) Conocimiento jurídico de la normativa de protección de datos

Estará familiarizado con las regulaciones y previsiones que afecten a su campo profesional o sector empresarial relacionados con la protección de datos:

- Derechos fundamentales y carta de derechos fundamentales de la UE, con referencia particular al derecho fundamental a la protección de datos personales.
- Principios básicos del RGPD y las normativas locales sobre protección de datos.
- Bases jurídicas de legitimación en el tratamiento de datos personales, Requisitos relacionados con la protección de datos al utilizar las TIC.
- Principios básicos del RGPD y las normativas locales sobre protección de datos.

b) Conocimiento en el ámbito de la Seguridad de la Información y las TIC

El DPO debe tener conocimientos técnicos básicos y comprender los problemas relacionados con las tecnologías de la información, y las medidas de seguridad que afectan a los sistemas:

- Organización del entorno TIC.
- Estructuras de sistemas, aplicaciones y procesos informáticos.
- Conocer los flujos de datos, incluyendo los Sistemas donde se produce el tratamiento de datos de carácter personal.
- Gestión de la seguridad de la información, basada en los objetivos de protección de la confidencialidad, integridad, disponibilidad y resiliencia.
- Identificación de riesgos para los sujetos de datos que resultan de los sistemas, aplicaciones y procesos TIC.
- Desarrollo de los controles y medidas de seguridad aplicables a los Sistemas de información para proteger los datos de carácter personal

8.4. Habilidades Personales

Además del conocimiento especializado en materia de protección de datos, resulta crucial las habilidades o softskills del DPO. Este tipo de habilidades sociales, key skills, o meta competencias tienen el denominador común de ser habilidades "transversales" e imprescindibles en cualquier DPO, máxime teniendo en cuenta su posición en la organización y las funciones atribuidas.

Este tipo de competencias, algunas innatas otras aprendidas, están relaciona- das con las competencias personales que cada individuo posee y gestiona a su manera, diferenciándolo de los demás en su carácter y comportamientos. Así podemos hablar de los siguientes tipos de habilidades:

1. **Introspectivas:** aprender a gestionar emociones, cambiar creencias limitadoras, identificar fortalezas y puntos de mejora, incrementar la autoconciencia y el sentido de autoeficacia.

2. **Diagnósticas y de acción:** planteamiento y resolución de problemas, examen de los recursos disponibles, creatividad, capacidad para afrontar situaciones nuevas y cambios profundos, flexibilidad, iniciativa, planificación, gestión del tiempo, etc.

3. **Relacionales:** empatía, escucha activa, asertividad, comunicación eficaz, gestión de conflictos, negociación y consenso, gestión y trabajo en equipo y liderazgo.

Sin duda, este tipo de competencias ayudan en la labor diaria de un DPO y deberían poco a poco irse incluyendo en la formación exigida tanto a nivel escolar como universitario y profesional. No cabe duda, que si acudimos al modelo de "las tres líneas de defensa" y declaración de posición al respecto del Instituto de Auditores Internos; se puede ver muy gráficamente la relación que un DPO tiene que hacer tanto de cara a la parte más operativa del negocio como con la parte de auditoría interna.

En este sentido, la capacidad que un DPO debe tener para coordinarse e interrelacionarse con áreas como compliance o seguridad de la información, además de con otros departamentos como TI, RR.HH., marketing, Desarrollo, Innovación, etc. viene mayoritariamente marcada por las referidas soft skills.

Igualmente, un DPO además de independiente y con "autoritas" suficiente dentro de su organización, debe ser una persona con un grado elevado de la ética tanto profesional como personal, íntegra (sin que hayan sido objeto de sanciones por infracciones del deber de secreto, de la normativa de protección de datos o condenados por delitos, especialmente los informáticos o de revelación de secretos), asertiva que sepa delegar y con capacidades para la comunicación (opiniones, posiciones, entendimiento de negocio y los diferentes intereses en juego) y la resolución de problemas.

Nuevamente, vemos que el hecho de tener un perfil jurídico o técnico no con- lleva per se el hecho de contar o reunir las referidas habilidades, por lo que un DPO puede recaer tanto en un perfil de corte jurídico o de corte técnico.

8.5. Formación

Sin duda, resulta elemental la formación continua del DPO y actualización permanente de sus conocimientos (modificaciones legales y jurisprudenciales, nuevas tecnologías, nuevos desarrollos técnicos, etc.)

En este sentido, el propio GT29 considera crucial el que las autoridades de protección de datos promuevan la formación adecuada y regular para los DPOs, como así ha hecho la Autoridad Española (AEPD) al aprobar el Esquema de certificación de delegados de protección de datos, donde se recogen las "competencias" requeridas a este puesto, tal y como se expone detalladamente en el apartado referido a la Certificación.

8.6. Deber de secreto

Según establece en el artículo 38.5 RGPD el DPO, con independencia de que sea de perfil técnico o jurídico, está obligado a mantener el secreto o la confidencialidad en lo que, respecto al desempeño de sus funciones, de conformidad con el derecho de la Unión o de los estados miembros.

Retos y desafíos

En su relación con el resto de las áreas de la organización, el DPO puede enfrentarse a una amplia gama de retos que dependerán del nivel de madurez de la organización en cuanto a su cultura de protección de datos. En organizaciones donde la privacidad y la protección de datos no están en el top de prioridades de la organización, es posible que el DPO puede percibir una falta de compromiso inicial que genere ciertas barreras importantes a la hora de desarrollar sus funciones.

A menudo, estas organizaciones perciben las normativas de privacidad como una carga adicional en lugar de una oportunidad para mejorar la confianza de los clientes o mejorar su competitividad en el mercado. El DPO, en este contexto, puede experimentar una falta de apoyo explícito por parte de la alta dirección o una resistencia pasiva por parte de otras áreas clave, que no ven el valor añadido de invertir tiempo y recursos en el cumplimiento normativo.

La resistencia a los cambios en las prácticas organizativas es uno de los obstáculos más comunes a los que se enfrenta cualquier DPO. Esta resistencia puede surgir de varios frentes: desde la falta de recursos hasta la percepción de que las medidas propuestas interferirán con la eficiencia operativa o la innovación. A menudo, la cultura organizativa preexistente no valora suficientemente la privacidad y, en algunos casos, puede haber un desconocimiento sobre las posibles sanciones o las implicaciones legales de no cumplir con las normativas de protección de datos.

Es en este escenario donde el DPO debe desplegar no solo sus conocimientos técnicos, sino también su habilidad para mediar y negociar. La clave es presentar el cumplimiento normativo no como una imposición, sino como un proceso que puede integrarse de manera armónica con los objetivos estratégicos de la organización. Este enfoque implica identificar áreas de riesgo y proponer medidas que no solo mitiguen

estos riesgos, sino que además aporten valor añadido, como mejoras en la eficiencia de los procesos o una mayor confianza de los clientes.

En las organizaciones más avanzadas, donde la protección de datos ya es parte de la cultura organizacional, los retos son diferentes, pero no menores. Aquí, el DPO puede encontrarse con un entorno de trabajo más colaborativo, donde las áreas están más familiarizadas con los principios de privacidad y seguridad. Sin embargo, el DPO debe estar preparado para gestionar nuevas complejidades, como la necesidad de mantenerse actualizado en un panorama normativo en constante cambio y con tecnologías emergentes y de rápida evolución como la inteligencia artificial.

Mejores prácticas

El éxito del DPO en su relación con las diferentes áreas de la organización está intrínsecamente ligado a su capacidad para construir y mantener alianzas sólidas. Estas alianzas no solo se basan en la confianza técnica del DPO, sino también en su habilidad para generar consenso y promover una cultura de cumplimiento proactiva. A continuación, se presentan tres aspectos clave que el DPO puede implementar para mejorar su efectividad y relación dentro de la organización:

1. Comunicación clara y adaptada

Una de las capacidades más críticas para el DPO es la habilidad de comunicar de manera clara y accesible. La naturaleza técnica y legal de la protección de datos puede resultar compleja para muchos dentro de la organización, desde los empleados que manejan datos en su día a día hasta los ejecutivos de alto nivel. Por ello, es esencial que el DPO no solo sea un experto y conozca profundamente la normativa la normativa, sino que sea capaz de transmitirla de forma comprensible y contextualizada, adaptando el mensaje a cada público. El éxito del DPO, en gran parte, depende de su capacidad para hacer que los aspectos técnicos y legales sean accesibles para todos, fomentando así una cultura de protección de datos en toda la organización.

El lenguaje jurídico y técnico asociado a la protección de datos puede ser denso y difícil de asimilar para quienes no están familiarizados con estos conceptos. Sin embargo, la protección de datos no es solo un tema para expertos legales o de TI, sino una responsabilidad compartida por todos los empleados de una organización. Desde el personal de atención al cliente que maneja información de contacto de los usuarios, hasta el equipo de recursos humanos que gestiona datos sensibles, todos deben entender cómo aplicar los principios de protección de datos en su trabajo diario.

Es aquí donde el DPO debe actuar como un traductor. Su función no es simplemente recitar artículos de la normativa, sino asegurarse de que cada área de la organización entienda qué implican esos requisitos en términos prácticos para sus actividades. Esto requiere no solo una comprensión profunda de la legislación, sino también la habilidad de simplificar y personalizar el mensaje para que sea relevante para cada equipo o individuo.

El primer paso para una comunicación efectiva es entender a la audiencia. Los diferentes niveles y áreas dentro de una organización requieren un enfoque de comunicación diferente. Por ejemplo, un equipo técnico de TI que gestiona los sistemas de seguridad y almacenamiento de datos necesitará información detallada sobre los requisitos específicos de seguridad, en términos de cifrado, autenticación y gestión de accesos. Por otro lado, el equipo de marketing podría necesitar orientación sobre cómo obtener y gestionar el consentimiento de los usuarios para el uso de sus datos personales.

En el caso de la alta dirección, por ejemplo, el DPO no debería centrarse en detalles técnicos, sino en los riesgos estratégicos y financieros que supone no cumplir con la normativa. Esto incluye las posibles sanciones, las implicaciones reputacionales y los beneficios a largo plazo de adoptar una cultura robusta de protección de datos. En cambio, cuando se trata de equipos operativos, la comunicación debe ser más práctica, explicando los procedimientos que deben seguirse en situaciones específicas, como la gestión de solicitudes de acceso o rectificación de datos.

De igual modo, es clave fomentar una comunicación bidireccional dentro de la organización. No se trata solo de transmitir instrucciones o recomendaciones, sino de crear un entorno donde las distintas áreas puedan plantear preguntas, expresar preocupaciones y compartir experiencias relacionadas con la protección de datos. Al promover este tipo de diálogo abierto, el DPO puede identificar posibles áreas de confusión o prácticas que necesitan mejorar. Para ello, el DPO puede establecer canales de comunicación accesibles, como por ejemplo un buzón de dudas o preguntas frecuentes.

Otro aspecto crítico de la comunicación clara es la simplificación de las políticas y procedimientos relacionados con la protección de datos. Muchas veces, los documentos de políticas son extensos, llenos de términos técnicos y escritos de manera que los empleados no pueden entender fácilmente lo que se espera de ellos. El DPO debe revisar y simplificar estos documentos, eliminando jerga innecesaria y explicando claramente los pasos que deben seguirse. Además, puede crear resúmenes ejecutivos o guías rápidas que resalten los puntos más importantes, para que los empleados tengan un recurso fácil de consultar cuando lo necesiten. Esto es especialmente útil para situaciones operativas en las que los empleados pueden tener poco tiempo para consultar largos documentos.

Por ejemplo, una guía rápida de "qué hacer en caso de una violación de datos" con pasos claros y directos puede ser mucho más efectiva que una política de 30 páginas. Al simplificar los procedimientos, el DPO asegura que el cumplimiento sea más accesible y que los empleados estén mejor preparados para actuar correctamente cuando sea necesario.

2. Capacidad de influencia y negociación

Una de las habilidades más relevantes que debe desarrollar un DPO es la capacidad de influencia y negociación. A menudo, el DPO no tiene autoridad jerárquica directa sobre los distintos departamentos de la organización, lo que significa que su efectividad depende de su capacidad para persuadir y negociar de manera eficaz. Esta habilidad es fundamental para lograr que las áreas de la empresa adopten e implementen las medidas necesarias para cumplir con las normativas de protección de datos, sin que ello genere fricciones innecesarias o se perciba como un obstáculo para la operación y los objetivos del negocio.

El DPO es, por definición, un rol independiente dentro de la organización. Esto significa que, aunque tenga la responsabilidad de asesorar, supervisar y garantizar el cumplimiento normativo, no siempre tiene el poder de tomar decisiones operativas o imponer cambios.

En organizaciones donde la cultura de protección de datos no está plenamente desarrollada o donde se percibe el cumplimiento normativo como una carga administrativa, el DPO puede enfrentar resistencia o, en el mejor de los casos, desinterés por parte de los responsables de otras áreas. Por lo tanto, su habilidad para negociar acuerdos, generar confianza y promover una colaboración transversal es esencial para su éxito.

La influencia del DPO no debe basarse únicamente en la presión normativa, sino en su capacidad para concienciar a los responsables de otras áreas sobre los beneficios de la protección de datos. Aquí, su autoridad proviene del conocimiento especializado que posee y de su habilidad para traducir ese conocimiento en beneficios tangibles para la organización.

Para ejercer una influencia efectiva, el DPO debe ser capaz de comunicar de manera clara y accesible cómo el cumplimiento normativo no solo protege a la organización de sanciones y riesgos legales, sino que también puede aumentar la confianza de los clientes, mejorar la eficiencia operativa y fortalecer la reputación de la empresa. Este enfoque requiere que el DPO tenga un conocimiento profundo tanto de la normativa como de los procesos y prioridades del negocio, para poder alinear sus recomendaciones con los objetivos estratégicos de la empresa.

Por ejemplo, en una organización que prioriza la experiencia del cliente, el DPO podría argumentar que implementar medidas robustas de protección de datos no solo cumple con la normativa, sino que también mejora la confianza de los consumidores y, en última instancia, su lealtad a la marca. Este tipo de argumentación, basada en la creación de valor añadido, es posiblemente más eficaz que simplemente insistir en la necesidad de cumplir con la ley.

En este proceso, el DPO también debe estar preparado para gestionar posibles conflictos entre las áreas de negocio y los requisitos normativos. Por ejemplo, si un área de la empresa presiona para el uso de datos personales con fines comerciales que no cumplen con los requisitos establecidos por la normativa de protección de datos, el DPO deberá ser firme en su posición, defendiendo los derechos

de los individuos y los principios de protección de datos, pero también proponiendo alternativas que permitan alcanzar los objetivos comerciales sin comprometer el cumplimiento. No se trata de trasladar únicamente el mensaje de "esto no se puede hacer", sino indicar que "esto lo debemos hacer de otra forma".

La capacidad de influencia del DPO se fortalece cuando logra fomentar una cultura de colaboración dentro de la organización. En lugar de ser visto como un fiscalizador externo que impone reglas, el DPO debe posicionarse como un aliado que facilita el trabajo de los departamentos mediante soluciones que simplifican el cumplimiento normativo.

Esta colaboración se puede fomentar creando canales de comunicación regulares entre el DPO y los diferentes equipos, para discutir problemas, aclarar dudas y trabajar juntos en la implementación de soluciones. El establecimiento de reuniones periódicas con los responsables de cada departamento para revisar el estado del cumplimiento puede ser una herramienta muy útil. El DPO debe asegurarse de que su enfoque sea proactivo y no solo reactivo ante los problemas.

De igual modo, es relevante que el DPO promueva la idea de que el cumplimiento de la normativa de protección de datos es una responsabilidad compartida por toda la organización, y no solo de su departamento. Fomentar la propiedad del cumplimiento a nivel departamental, mediante la designación de responsables de privacidad en cada área, puede facilitar la comunicación y la implementación de medidas correctivas cuando sea necesario.

3. Conocimiento del negocio y del sector

El DPO debe posicionarse como un facilitador que colabora activamente con las distintas áreas de la organización para asegurar que el cumplimiento de la normativa de protección de datos no se vea como una imposición, sino como un aspecto que fortalece la eficiencia, la innovación y la competitividad del negocio.

Un conocimiento profundo del negocio y del sector en el que opera la organización permitirá al DPO adaptar sus recomendaciones y medidas de cumplimiento a la realidad operativa de la empresa. De este modo, se minimizan las interrupciones en los procesos y se integran las medidas de protección de datos en la propia estructura y cultura organizativa.

Una de las primeras tareas del DPO debe ser familiarizarse con los objetivos estratégicos de la organización. Es decir, debe comprender cuál es la misión de la empresa, sus prioridades de negocio, los productos o servicios que ofrece, sus mercados y clientes, así como los retos y oportunidades a los que se enfrenta. Con esta comprensión, el DPO podrá ajustar su enfoque de cumplimiento para que esté alineado con el contexto en el que se desenvuelve la organización y en el que operan las diferentes áreas.

9 EL DPO EN EL MARCO NORMATIVO DE LA INTELIGENCIA ARTIFICIAL

9. 1. Introducción

El recientemente publicado Reglamento 2024/1689 del Parlamento europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante, el **"Reglamento de Inteligencia artificial"** o **"RIA"**), ha abierto un debate en el mundo profesional y académico en relación con su aplicación en muchos aspectos. Para los profesionales de la protección de datos, uno de los que sin duda más debates está centrando, es el de la figura del delegado de protección de datos (DPO) y cuál debe ser su papel en el marco de lo dispuesto por esta nueva normativa.

Por su parte, las autoridades de protección de datos, hasta el momento, han ido publicando guías en las que abordan cómo debe cumplir esta tecnología con el Reglamento General de Protección de Datos (RGPD) para el caso de que los tratamientos de datos personales a realizar la incorporen o, para el caso de que la creación de la propia tecnología implique un tratamiento de datos.

La inteligencia artificial -como otras tecnologías- se configura, en el mundo de la protección de datos, como un medio más a disposición de responsables y encargados del tratamiento que deben decidir, si y en qué términos, se incorpora a sus procesos.

Con el RIA ya publicado y en el periodo de gracia que concede para su aplicación, ya tenemos claro el mapa de requerimientos que estos sistemas van a tener que cumplir, usen o no datos personales, así como las medidas transversales de las que se deben dotar las organizaciones para analizar, detectar y mitigar sus riesgos.

En cuanto al DPO, es necesario señalar que el RIA no establece ni configura una figura análoga, aspecto que -como sabemos y hemos visto a lo largo de esta II Edición del Libro Blanco del DPO-, el RGPD sí que hace y de forma detallada en sus artículos 37 (designación), 38 (posición) y 39 (funciones).

En este contexto, en el apartado 7 de esta Guía, vamos a exponer las claves que entendemos que las organizaciones deberían valorar para concluir la asignación o no de nuevas responsabilidades en torno a la Inteligencia artificial al DPO y en tal caso cuáles. Para ello, a continuación, se abordan las principales obligaciones que trae consigo el RGPD, así como el RIA y, para cada una de las mismas, se analiza la posibilidad o no de complementar los circuitos establecidos para el RGPD para asegurar el cumplimiento del RIA.

Con carácter previo a estas obligaciones, abordaremos la **definición del rol del DPO en el RGPD** y dos cuestiones transversales que entendemos que impactan en todo este análisis como son la coincidencia de **objetivos y la complementariedad de textos normativos (RGPD y RIA).**

9. 2. La definición del rol del DPO en la normativa de protección de datos

Con carácter previo a determinar qué roles y responsabilidades podemos atribuirle al DPO en el ámbito de la IA debemos tener en cuenta cuáles son las funciones que la normativa de protección de datos les atribuye a los efectos de poder valorar la asignación de otras funciones en virtud de una tercera normativa (RIA) y discernir si resulta compatible y deseable o, en cambio, podría suponer un conflicto de interés.

En este sentido, recodemos que el art. 39 RGPD atribuye al **DPO las funciones de**:

- **Informar y asesorar** al responsable de las obligaciones en materia de protección de datos,qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos,
- **Supervisar** el cumplimiento esta normativa,
- **Ofrecer** asesoramiento en las evaluaciones de impacto y supervisar su aplicación,si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y
- **Cooperar** con la autoridad de control y actuar como punto de contacto

Adicionalmente, el art. 38 RGPD establece que:

- los interesados podrán ponerse en contacto con el DPO por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos.

9.3. Objetivos coincidentes de los marcos normativos de protección de datos e inteligencia artificial

Según el art. 1.2 del RGPD…

- *[…] El presente Reglamento* **protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.**

Por su parte, el art. 1 del RIA establece que…

- *[El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un* ***elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta,*** *incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, «sistemas de IA») en la Unión así como prestar apoyo a la innovación.*

De la literalidad de los artículos citados y de la práctica que acumula el RGPD y las resoluciones tanto de las autoridades de protección de datos como del Tribunal de Justicia de la Unión Europea, el RGPD hasta ahora -y por lo que parece en un futuro el RIA- se configuran como normas que establecen obligaciones y mecanismos para proteger los derechos establecidos en la Carta de derechos fundamentales de la Unión.

Así lo ha demostrado la práctica de las autoridades de protección de datos tanto a nivel nacional como europeo y lo exponen de manera muy clara Alessandro Mantelero y Maria Samantha Esposito en su artículo An Evidence-based methology for human rights impact assessment in the development of AI data-intensive systems cuando utilizan justamente esas resoluciones como base de la que partir para descubrir como la inteligencia artificial puede afectar a los derechos fundamentales[18] .

9. 4. RGPD y RIA: la complementariedad de los textos normativos

La lectura conjunta de ambas normas y sobre todo lo dispuesto en los considerandos del RIA nos llevan a concluir que existe una complementariedad normativa.

De acuerdo con el considerando 9 y 10 el RIA, sus previsiones:

- ***[…] deben entenderse sin perjuicio del Derecho vigente de la Unión, en particular en materia de protección de datos,*** *protección de los consumidores, derechos fundamentales, empleo, protección de los trabajadores y seguridad de los productos, al que* ***complementa el presente Reglamento".***

- ***[…] deben facilitar la aplicación efectiva y permitir el ejercicio de los derechos y otras vías de recurso de los interesados garantizados por el Derecho de la Unión en materia de protección de datos personales, así como de otros derechos fundamentales".***

Esta complementariedad e instrumentalidad del RIA para el cumplimiento del RGPD se va detallando a lo largo del texto del RIA, por ejemplo, en lo relativo a la definiciones o conceptos como el de perfilado (art. 4.4 RGPD), perfilado que se establece como determinante para que un sistema sea de alto riesgo de acuerdo con lo previsto en el art. 6.3 in fine.

Repasada la configuración del DPO en el RGPD y vista la coincidencia de objetivos así como la complementariedad entre el RGPD y el RIA, se abordan en los siguientes apartados las obligaciones principales del RGPD y para cada una de ellas se señalan las que del RIA se entienden puede tener sentido incluir en los circuitos y estructuras ya creados.

[18] https://www.sciencedirect.com/science/article/pii/S0267364921000340
https://www.sciencedirect.com/science/article/pii/S0267364924000864

a) Registro de Actividades de Tratamiento e Inventario de sistemas de IA:

El gobierno de los sistemas de IA pasa, sin duda, por su inventario y calificación en función del riesgo. Sin ello, no les resultará posible a las organizaciones determinar el ámbito de aplicación de la norma ni las obligaciones a cumplir.

En este sentido, si bien es cierto que el RIA no establece una obligación de inventario como tal de los sistemas de IA, sí establece obligaciones de registro de los sistemas de alto riesgo en la base de datos del CE[19] y concreta la información que deberá presentarse para ello[20].

Por su lado, la normativa de protección de datos sí positiviza la obligación de tener y mantener un registro de actividades del tratamiento con un cierto contenido (art. 30 RGPD), para el cual la AEPD ya ha establecido en sus guías que el mismo debe tener identificados los activos que soportan el tratamiento y, en particular, los sistemas de IA que se incluyan, si es que se utilizan.

Con ello, resulta conveniente valorar si el RAT del art. 30 RGPD puede ser la base sobre la que construir el inventario de IA o resulta mejor crear dos registros teniendo en cuenta ciertas variables:

i. Las autoridades de protección de datos consideran la IA como un medio (activo) del tratamiento de datos que puede ocasionar riesgos específicos al mismo y cuya introducción debe valorarse desde un punto de vista de necesidad, idoneidad y proporcionalidad en sentido estricto. Incorporar estos activos y su cadena de suministro puede ser una herramienta para gobernar el cumplimiento y hacer una gestión de riesgos adecuada.

ii. El tratamiento de datos personales por parte de la organización: sin duda organizaciones que tengan grandes tratamientos de datos y desarrollen o usen IA parece más razonable usar este registro que otras donde no se traten este tipo de datos.

iii. Tratamiento de datos personales y sistema de IA de alto riesgo: las organizaciones deben tener en cuenta que los sistemas de IA que se categorizan como alto riesgo de acuerdo con el art. 6 del RIA se concretan en los anexos I y III. En particular, resulta difícil imaginar sistemas de IA que tengan cabida en el Anexo III y que no supongan un tratamiento de datos personales (Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones o Empleo, gestión de los trabajadores y acceso al autoempleo).

b) Enfoque a riesgos:

El RGPD en palabras de la AEPD "demanda la identificación, evaluación y mitigación, realizadas de una forma objetiva, del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales. La mitigación ha de realizarse mediante la adopción de medidas técnicas y organizativas que garanticen y, además, permitan demostrar la protección de dichos derechos. Estás deberán determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento. Además, dichas medidas se revisarán y actualizarán cuando sea necesario. En definitiva, el RGPD exige un proceso de gestión del riesgo para los derechos y libertades de los interesados"[21] .

Por su lado, la normativa de protección de datos sí positiviza la obligación de tener y mantener un registro de actividades del tratamiento con un cierto contenido (art. 30 RGPD), para el cual la AEPD ya ha establecido en sus guías que el mismo debe tener identificados los activos que soportan el tratamiento y, en particular, los sistemas de IA que se incluyan, si es que se utilizan.

[19] *Artículo 49. Registro y Artículo 71. Base de datos de la UE para los sistemas de IA de alto riesgo enumerados en el ANEXO I*

[20] *Anexo VIII del RIA*

[21] *Guía de la AEPD, Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, de Junio 2021*

Concreta el RGPD este riesgos para los derechos y libertades de las personas físicas, entre otros en su considerando 75 cuando establece que *"pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados".*

El RIA por su parte exige en su art. 9 el establecimiento de un sistema de gestión de riesgos en relación con los sistemas de IA de alto riesgo para la salud, la seguridad o los derechos fundamentales. Dicho artículo concreta a su vez las etapas que debe tener dicho proceso iterativo, etapas que coinciden con la gestión de riesgos que se realiza en el mundo de la protección de datos.

De hecho, en este caso el propio RIA incluye una previsión en el apartado 10 de dicho artículo cuando establece que esta gestión de riesgo puede formar par de los procedimientos de gestión de riesgos establecidos con a arreglo a otras disposiciones del derecho de la unión.

Resultará, por tanto, relevante en este punto que las organizaciones analicen si están en este último caso y si disponen ya de sistemas de gestión de riesgos para incluir las previsiones del RIA.

En este sentido, los circuitos y roles y responsabilidades creados y asignados en materia de protección de datos pueden ser, sin duda, una ubicación con muchas sinergias, teniendo en cuenta que:

i. Los procesos de gestión de riesgos que contemplan ambas normas resultan equivalentes.
ii. Los riesgos que persiguen identificar tienen un objetivo común: garantizar los derechos fundamentales.
iii. Los DPO y los equipos que actualmente realizan están tareas en materia de protección de datos tienen el conocimiento y la experiencia acumulada de estos años .

c) Evaluaciones de impacto en protección de datos y evaluaciones de impacto en derechos fundamentales (PIA y FRIA) :

El RGPD establece en su **art. 35 la obligación de realizar una PIA** en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas. Esta evaluación consiste en **evaluar "en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo.** *El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el*

fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento".

Por su parte el art. 27 del RIA, exige la realización de una evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo (FRIA) para los responsables del despliegue que consistirá en:

> **iv.** una descripción de los procesos del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista;
>
> **v**. una descripción del período de tiempo durante el cual se prevé utilizar cada sistema de IA de alto riesgo y la frecuencia con la que está previsto utilizarlo;
>
> **vi.** las categorías de personas físicas y colectivos que puedan verse afectados por su utilización en el contexto específico;
>
> **vii.** los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y colectivos determinadas con arreglo a la letra c) del presente apartado, teniendo en cuenta la información facilitada por el proveedor con arreglo al artículo 13;
>
> **viii.** una descripción de la aplicación de medidas de supervisión humana, de acuerdo con las instrucciones de uso;
>
> **ix.** las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación.

En este caso, la complementariedad de ambas obligaciones queda recogida en el RIA en concreto en el art. 27.4 cuando establece que *"Si ya se cumple cualquiera de las obligaciones establecidas en el presente artículo mediante la evaluación de impacto relativa a la protección de datos realizada con arreglo al artículo 35 del Reglamento (UE) 2016/679 o del artículo 27 de la Directiva (UE) 2016/680, la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 del presente artículo complementará dicha evaluación de impacto relativa a la protección de datos".*

En cuanto a la publicidad de estos ejercicios (PIAS y FRIAS) cabe tener en cuenta que si bien en el mundo de la protección de datos no es una obligación ha sido reconocido por las autoridades supervisoras como una buena práctica. En el ámbito del RIA, en cambio, se ha establecido la obligación para los responsables del despliegue de incluir en el registro de la CE según el art. 49.3 y el Anexo VIII *"[…] 4. Un resumen de las conclusiones de la evaluación de impacto relativa a los derechos fundamentales realizada de conformidad con el artículo 27. 5. Un resumen de la evaluación de impacto relativa a la protección de datos realizada de conformidad con el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680, tal como se especifica en el artículo 26, apartado 8, del presente Reglamento, cuando proceda."*

Con estas previsiones parece lógico que las organizaciones "reutilicen", si es que los tienen, los circuitos y los roles y responsabilidades establecidos en el mundo de la protección de datos para la realización de las requeridas FRIAS. Teniendo en cuenta eso sí las evoluciones que serán necesarias para cumplir con los requisitos del mencionado art. 27 RIA de acuerdo con las instrucciones que publique la Oficina de IA.

d) Notificación de brechas personales y notificación de incidentes graves:

El RIA establece la **obligación de notificación de incidentes graves**, a los proveedores o los responsables de despliegue cuando sean quienes adviertan el mismo, cuando se haya establecido un vínculo causal entre el sistema de IA y el incidente grave o la probabilidad razonable de que exista dicho vínculo y, en cualquier caso, a más tardar quince días después de que el proveedor o, en su caso, el responsable del despliegue, tengan conocimiento del incidente grave.

Se define como incidente grave **un incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga alguna de las siguientes consecuencias:**

- el fallecimiento de una persona o un perjuicio grave para su salud;
- una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas;
- el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales;
- daños graves a la propiedad o al medio ambiente;

Establece una especificidad el RIA en el caso de los **sistemas de IA de alto riesgo a que se refiere el anexo III,** introducidos en el mercado o puestos en servicio por proveedores que estén **sujetos a instrumentos legislativos de la Unión por los que se establezcan obligaciones de información equivalentes** a las establecidas en el presente Reglamento, cuando establece que la notificación de estos incidentes se limitará a aquellos derivados del incumplimiento de obligaciones en virtud del derecho de la unión destinadas a proteger los derechos fundamentales.

Parece claro, en este punto, que las organizaciones deberán velar porque este nuevo procedimiento que garantice que se comunican los incidentes graves se incardine en los procedimientos ya existen teniendo en cuenta:

i. las organizaciones que ya estén sujetas a otras normas cuyo cumplimiento les obligue a comunicar alguno de estos fenómenos tendrán procedimientos establecidos adicionales o no a los derivados de la normativa de protección de datos pero no sólo (piénsese por ejemplo en DORA u otras normativas)Los riesgos que persiguen identificar tienen un objetivo común: garantizar los derechos fundamentales.

ii. los circuitos establecidos con motivo del cumplimiento del art. 33 RGPD están ya garantizando la valoración de brechas de datos personales a efectos de comunicación a las autoridades de supervisión cuando sea probable que exista un riesgo para los derechos fundamentales.

iii. de los 4 factores que configura el RIA como incidente grave parece a priori que el más difícil de valorar será justamente el que tenga como consecuencia *el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales.*

iv. la notificación realizada en el ámbito del RIA a la autoridad de mercado derivadas del incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales, será comunicada por estas autoridades a las autoridades encargadas de proteger los derechos fundamentales (entre las cuales estarán las autoridades de protección de datos).

v. el proceso de gestión y comunicación establecido por el RIA es equivalente al establecido por el RGPD.

En contexto, parece también claro que será deseable aprovechar los circuitos, los roles y responsabilidades y la experiencia acumulada de estos años en determinar la afectación a los derechos fundamentales a efectos de riesgos y comunicación.

e) Obligaciones de transparencia e información:

El art. 50 RIA establece obligaciones de transparencia e información para los sistemas de IA que interactúen con personas, realicen ultra falsificaciones, hagan reconocimiento de emociones o categorización biométrica. En concreto,

i. obligan a informar al usuario que está interactuando con un sistema de IA o que su contenido ha sido generado por el mismo.Los circuitos establecidos con motivo del cumplimiento del art. 33 RGPD están ya garantizando la valoración de brechas de datos personales a efectos de comunicación a las autoridades de supervisión cuando sea probable que exista un riesgo para los derechos fundamentales.

ii. deben cumplir de *"manera clara y distinguible a más tardar con ocasión de la primera interacción o exposición"..*

Adicionalmente, el art. 13 del RIA cuando establece las obligaciones de transparencia y comunicación de información indicando la necesidad de que los proveedores de sistemas de IA cuenten con unas instrucciones de uso que contengan una mínima información (tales como la finalidad prevista del sistema, el nivel de precisión, los riesgos, etc.).

Estas obligaciones de transparencia y su configuración resultan paralelas y permiten y posibilitan el cumplimiento de las obligaciones de transparencia e información que establecen los arts. 12 (transparencia de la información, comunicación y modales de ejercicio de los derechos de los interesados), y 13 y 14 (información que deberá facilitarse a los titulares de los datos cuando se obtengan o no del interesado), a saber y entre otras, finalidad, lógica y consecuencias de los perfilados y de los tratamientos, derecho a obtener una intervención humana para las decisiones automatizadas, etc.

f) Derechos de los titulares de los datos / afectados:

Además de los derechos de información, el RGPD recoge otros derechos para los titulares de los datos que confluyen con los reconocidos por el RIA. En este sentido:

a. Derecho a no ser objeto de decisiones automatizadas (art. 22 RGPD) y Derecho a obtener una explicación de decisiones tomados individualmente (art. 86 RIA)

El art. 22 del RGPD establece el derecho a no ser objeto de una decisión automatizada y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna.

El art. 86 del RIA por su parte establece el derecho a obtener una explicación cuando la decisión se base en los resultados de salida de la IA de alto riesgo y cuando dicha decisión produzca efectos jurídicos o afecte significativamente de modo similar a dichas personas de manera que tenga un efecto negativo en su salud, su seguridad o sus derechos fundamentales.

Con ello, entendemos que las organizaciones deben tener en cuenta i) los circuitos que tienen establecidos en el ámbito del RGPD para detectar este tipo de decisiones y ii) facilitar los derechos oportunos incluyendo la información y procesos necesarios. Esos circuitos pueden ser los que aseguren el cumplimiento de lo previsto en el RIA (permiten sinergias, evitan incoherencias).

b. Derecho a presentar una reclamación ante la autoridad de control (art. 77 RGPD) y Derecho a presentar una reclamación ante la autoridad de vigilancia del mercado (art. 85 RIA)

En el mismo sentido, ambos artículos reconocen estos derechos a favor de los afectados. Y sirven, a nuestro entender, las conclusiones del apartado anterior.

g) Obligaciones para los sistemas de IA de alto riesgo y principios de protección de datos:

El RIA establece una serie de obligaciones concretas para cada uno de los sistemas de IA de alto riesgo y que se concretan en

* datos y gobernanza
* documentación técnica
* conservación de registros
* transparencia y comunicación de información a los responsables del despliegue
* supervisión humana
* precisión, solidez y ciberseguridad

Estos requisitos concretos y que deben incluirse desde una perspectiva técnica en el diseño de los sistemas de IA de alto riesgo, estaban en cierta manera implícitos en la aplicación de la normativa de protección de datos y, en concreto, en el art. 5 del RGPD al establecer que los datos personales serán (señalamos para cada uno de ellos su correspondencia con las obligaciones expuestas del RIA anteriormente, en cursiva):

a. Tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia») **->** *datos y gobernanza en lo que se refiere al control del sesgo*

b. Recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; («limitación de la finalidad»);

c. **Adecuados, pertinentes y limitados** a lo necesario en relación con los fines para los que son tratados («minimización de datos»); **->** ***precisión****, solidez y ciberseguridad*

d. **Exactos y, si fuera necesario, actualizados;** se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); **->** ***datos y gobernanza, precisión, solidez*** *y ciberseguridad*

e. Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; («limitación del plazo de conservación»);

f. Tratados de tal manera que se garantice una ***seguridad adecuada*** de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad») ***precisión, solidez y ciberseguridad***

g. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»). ***transparencia y comunicación de información a los responsables del despliegue (instrucciones de uso, registro de logs, etc.)***

Adicionalmente, en lo que respecta a la documentación técnica y al registro de logs, el principio de protección de datos por defecto y desde el diseño y su cumplimiento es uno de los que referencian las autoridades supervisoras de protección de datos cuando el funcionamiento de los sistemas no es correcto. En cuanto a la supervisión humana, nos remitimos a los comentarios incluidos en el apartado anterior.

9.5. Conclusiones

El RGPD y el RIA persiguen objetivos coincidentes y se configuran en gran manera como normas complementarias.

Tanto el DPO como los distintos profesionales que cada día se dedican a la protección de datos se encuentran, sin duda, en una posición en la que pueden aportar sus conocimientos especializados en el ámbito del nuevo Reglamento de Inteligencia Artificial y la experiencia acumulada en estos años.

Los circuitos, las estructuras, procedimientos y normas, así como los roles y responsabilidades atribuidos con motivo de la implementación del RGPD pueden ser el punto de partida ideal para la implementación del RIA.

Crear estructuras paralelas a las establecidas en protección de datos en organizaciones con protagonismo del uso de datos personales puede, además de convertirse en redundante, llevar a incoherencias dentro y fuera de la organización.

La formación continua que siempre ha sido necesaria en el ámbito de la protección de datos se convierte en el entorno de la IA en un reto aún mayor.

La figura del DPO se ha configurado con mucho detalle en el RGPD. La atribución de responsabilidades en el mundo de la IA si la Organización así lo desea debe seguir un camino paralelo y cuidadoso. Atribuir funciones diferentes a las establecidas por el RGPD requerirá de un estudio minucioso para evitar conflictos de interés. La posición en la que coloca el RGPD al DPO permite, desde un primer momento, colocar la implementación del RIA en la alta dirección y su conseguir su necesario compromiso.

Categoría	Métrica	Detalles/Objetivo
1. GOBIERNO DE LA PRIVACIDAD - Normas internas (Políticas, Procedimientos y Protocolos de actuación en Protección de datos)	Nº total de normas corporatvas	Realizar un inventario de documentos que conforman la normativa interna, actualizado periódicamente, con control de versiones, que muestre el número total de la muestra
	Nº de normas corporativas revisadas	Establecer ciclos de revisión periódica, para el control del contenido, que contemple eventos de actualización extraordinarios (Ej. Publicación de una nueva norma).
	Nº de normas corporativas actualizadas o de nueva creación	De las normas corporativas revisadas cuántos han requerido actualización o elaboración *ex novo*
	Nº de Procedimientos aprobados	Cuántos nuevos procedimientos se han aprobado, con contenido parcial o total de protección de datos, y referencia a su propósito o necesidad
2. ACCIONES DEL DPD - Nombramientos, Consultas e Interacciones con la Autoridad de Control	Nº de figuras/personas asignadas al cumplimiento en protección de datos	Indicardor del número de figuras nombradas en la Organización y/o personas asignadas al asesoramiento y/o supervisión del cumplimiento de la normatia de protección de datos personales
	Nº de Requerimientos de Información recibidos	Evaluar la capacidad de la organización para gestionar satisfactoriamente los requerimientos de las autoridades de control
	Nº de requerimientos de información archivados por la Autoridad de Control	
	Nº de Consultas previas relacionadas con DPIAs	
	Nº de Consultas del DPD a la Autoridad de Control	
	Nº de Procedimientos sancionadores abiertos por la Autoridad de Control	
	Nº de Procedimientos sancionadores cerrados sin sanción	
	Nº de Procedimientos sancionadores que finalizan en sanción	
	Importe anual de las sanciones recibidas	
	Nº de certificaciones o recertificaciones en las que el DPD ha participado	Participación en certificaciones y estándares
3. LICITUD Y TRASPARENCIA - Deber de Información, licitud y gestión del consentimiento	Nº total de cláusulas informativas vigentes	Realizar un inventario del clausulado, actualizado periódicamente, con control de versiones, que muestre el número total de la muestra
	Nº de cláusulas de privacidad revisadas	Establecer ciclos de revisión periódica, para el control del conentido, que contemple eventos de actualización extraordinarios (Ej. Creación de una nueva página web)
	Nº de cláusulas de privacidad actualizadas o de nueva creación	Del clausulado revisado cuántas requirieron actualización o elaboración ex novo
	Nº Consentimientos para actividades de tratamiento	Evaluar claridad y accesibilidad de mecanismos de consentimiento
	Consentimiento para Compartir Datos con terceras partes	Revisar y actualizar regularmente las políticas de compartición
	Consentimiento Opt-in para actividades de Marketing	Medir la tasa de aceptación y ajustar estrategias según sea necesario
	Número de LIAs Realizadas	Cumplimiento de ejercicio de ponderción sobre actividades de tratamiento que lo requieran
4. GESTIÓN DE DERECHOS - Gestión de los derechos y reclamaciones realizados por los interesados	Nº de ejercicios de derechos recibidos	Incluir categorización por tipo de solicitud (acceso, supresión, oposición, etc.)
	Nº de ejercicios de derechos en progreso	Detallar razones de cierre (cumplidas, denegadas, etc.)
	Nº de ejercicios de derechos archivados / cerrados	Incluir plazos estimados de resolución
	Nº de ejercicios de derechos contestados fuera de plazo	Control de los derechos contestados fuera de plazo y análisis de las causas
	Nº de Reclamaciones recibidas no categorizadas como ejercicio de derechos	Inventario de las reclamaciones de los interesados recibidas, que no tienen por objeto el ejercicio de un derecho
	% indicidencias	Interesados que consideran que su derecho no ha sido atendido de forma correcta
	% tramitadas en tiempo requerido	Tramitación dentro del plazo legal establecido por el RGPD
5. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO - Participación del DPD en la gestión de nuevas iniciativas	Nº de proyectos comunicados al DPD	Medir el soporte y asesoramiento proporcionado a los equipos
	% de proyectos viables	
	Nº de proyectos detectados que no han sido comunicados al DPD	Detalles sobre la naturaleza y alcance de los proyectos
6. REGISTRO DE ACTIVIDADES DE TRATAMIENTO - Gestión y actualización del RAT	Nº de actividades de tratamiento, realizadas como Responsable, totales	Medir evolución de las actividades de tratamiento y tendencias
	Nº de actividades de tratamiento, realizadas como Encargado, totales	
	Nº de actividades de tratamiento, realizadas como Responsable, nuevas	
	Nº de actividades de tratamiento, realizadas como Encargado, nuevas	
	Nº de actividades de tratamiento que han dejado de realizarse	
	% de crecimiento o decrecimiento del volumen de actividades de tratamiento	
7. ANÁLISIS DE RIESGOS Y EIPD - Análisis del riesgo y el impacto para los derechos de los interesados	% de tratamientos con el AARR realizado	Número de AARR realizados / pendientes respecto al número de finalidades de tratamiento inventariadas en el RAT
	Nº de tratamientos con nivel de riesgo inherente Alto / Muy alto	Monitorización del nivel de riesgo
	Nº de tratamientos con nivel de riesgo residual Alto / Muy alto	
	Nº de DPIAs Requeridas	Analizar la proporción de DPIAs en relación a las actividades totales de tratamiento
	Nº de PIAs/DPIAs Completadas	Medir el soporte y asesoramiento proporcionado a los equipos
	Tiempo total invertido (en horas de trabajo)	Evaluar eficiencia y efectividad en la realización
8. INCIDENTES DE SEGURIDAD Y BRECHAS DE DATOS PERSONALES - Gestión de los incidentes sobre los datos personales	Nº de Incidentes comunicados como brecha	Número de comunicaciones frente a brechas
	Nº de Incidentes que materializan en brecha de datos personales	Número de brechas de datos personales y clasificación por naturaleza (pérdida de datos, acceso no autorizado, etc.)
	Nº de brechas por Severidad	Definir niveles de severidad (bajo, medio, alto)
	Nº de brechas por Unidad de Negocio	Identificar áreas con mayor riesgo
	Nº de Interesados Afectados (totales)	Estimar el impacto en usuarios
	% de brechas cerrados satisfactoriamente	Evaluar la eficacia de las medidas de contención
	% de brechas con Causa raíz / vector de entrada Identificada	
	Nº de brechas Notificadas a la Autoridad de control	
	% de expedientes de brechas archivados por la autoridad de control tras la comunicación	
	Nº de brechas Notificados a Interesados	
	Tiempo Medio de Descubrimiento	Medir eficacia de sistemas de detección
	Tiempo Medio de Resolución	Evaluar eficiencia de procesos de respuesta y remediación
	Nº de brechas de brechas de datos notificados por terceras partes	Número de incidentes, con afectación a datos personales, originados en la cadena de suministro y notificados a la Organización

9. MEDIDAS DE SEGURIDAD - Gestión de los controles y medidas para garantizar la seguridad de los datos personales	Nº de sistemas de información que alojan o tratan datos personales	Monitorización de los controles y medidas de seguridad sobre los sistemas de información, tanto automatizados no automatizados, que alojan o tratan datos personales, así como de los plazos de conservacióndne dichos datos
	Nº de revisiones / auditorías realizadas sobre la eficacia de los controles en los sistemas de información en materia de seguridad de los datos personales	
	Nº de procesos de conservación y borrado realizados sobre los datos personales	
10. ACCOUNTABILITY Y FORMACIÓN - Cumplimiento del principio de responsabilidad proactiva, trazabilidad y formación	Nº de formaciones impartidas	Desglosar métodos (en línea, presencial)
	Nº Empleados convocados	Segmentar por departamento y rol
	% de Empleados que realizan formación	Medir efectividad de la acción
	% de Empleados que superan formación	Adaptar contenido formativo según resultados
	Nº de acciones de concienciación desplegadas	Establecer metas futuras y comparar con desempeño pasado
	Nº de acciones de concienciación a la Alta Dirección	Formaciones y acciones de concienciación impartidas a la Alta Dirección en materia de datos personales
	Nº de controles llevados a cabo por el DPO para la supervisión del cumplimiento	Nivel de monitorización del DPD a través de la realización de controles periódicos
	Nº de controles ineficaces	Número de controles que han tenido un resultado no suficiente conforme a lo establecido por la normativa y por la Organización
11. ENCARGOS DEL TRATAMIENTO - Gestión de la tercera parte o cadena de suministro, y de los tratamientos realizados como encargados del tratamiento	Nº Contratos con terceros [NDA / Contrato de Cesión / Contratos sin acceso a datos, etc]	Volumen total de contratos en los que el DPD ha participado con terceras partes
	Nº de Contratos Intragrupo (si aplica)	Volumen de contratos de protección de datos entre entidades del Grupo de la Organización
	Nº Contratos de Encargo de Tratamiento	Volumen de encargos de tratamiento
	Plazos para Cierre	Evaluar alineación con estándares internos
	Nº de terminación de prestaciones de servicios con acceso a datos (encargados) y devolución / destrucción segura de la información personal acreditada mediante certificado	Monitorizar el volumen de información en posesión de terceros tras la terminación de los servicios
	Nº de homologaciones completadas	Evaluar la debida diligencia sobre la cadena de suministros
	Nº de rehomologaciones completadas	
	% Proveedores que han superado las evaluaciones	
	Nº de auditoría de terceros durante el tiempo de vigencia del contrato para asegurar el cumplimiento de las medidas de protección de datos	
	Nº Solicitudes de homologación recibidas y completadas	Incluir detalles sobre aspectos evaluados
	% satisfactorios	Evaluar la capacidad de la empresa para cumplir con lo requerido
	Plazo promedio para su tramitación	Evaluar plazos de tramitación
12. TRANSFERENCIAS INTERNACIONALES DE DATOS - Gestión de las TID y evaluación de las TIA	Nº de TIAs Realizadas	Seguimiento post-Schrems II y cumplimiento de nuevas normativas
	Nº de TID legitimadas	
	Nº de TID realizadas sin las garantías adecuadas	
13. CORRESPONSABILIDAD DE LOS DATOS PERSONALES - Gestión de la corresponsabilidad con terceras organizaciones	Nº de relaciones de Corresponsabilidad	Control de las relaciones de corresponsabilidad con terceros
	Nº de relaciones de Corresponsabilidad nuevas gestionadas	

FEBRERO 2025

II EDICIÓN DEL LIBRO BLANCO DEL DPO

@ISMSForum