EL LIBRO BLANCO DEL DPO

Una iniciativa de

isms forum spain

dpi Data Privacy Institute

EL LIBRO BLANCO | DEL DPO

Dirección y coordinación:

CARLOS A. SAIZ, Director del Data Privacy Institute de ISMS Forum
BERTA BALANZATEGUI, Privacy Counsel de GE Corporation

Colaboradores:

Araceli Fernández
Elena Mora
Gemma Sánchez
Gonzalo Erro
Javier Lomas
Josep Bardallo
Manel Leal
Óscar Sánchez
Pilar Pascual
Susana Rey
Xavier Vila

Revisores:

ANTONIO MUÑOZ MARCOS
PABLO MARTÍNEZ

Editor:

DANIEL GARCÍA SÁNCHEZ, Director General de ISMS Forum.

Diseño y maquetación:

CYNTHIA RICA GÓMEZ, Responsable de comunicación de ISMS Forum.

ÍNDICE

I INTRODUCCIÓN Y CONTEXTO ACTUAL

I.1.- Marco normativo.

Ya la derogada Directiva 95/46/CE hacía referencia a la figura del DPD bajo la denominación de encargado de los datos personales en relación con la excepción de la obligación de notificación de los ficheros a la autoridad de control, dando oportunidad así a los Estados Miembros a la inclusión de esta figura en la normativa nacional, cosa que en España no se hizo -donde se había optado por la figura obligatoria del Responsable de Seguridad- con unas atribuciones y un foco de actuaciones diferente.

Ya en el momento actual, la primera e inevitable referencia legislativa relativa al DPD 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.

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, perfilan y completan lo regulado en RGPD en relación con esta figura.

Asimismo, debemos añadir a estas referencias normativas las Directrices WP243 del Grupo de Trabajo del Artículo 29 ("GT29", hoy ya extinto) sobre los Delegados de Protección de Datos, cuya versión de 5 de abril de 2017 ha sido refrendada por su sucesor, el European Data Protection Board ("EDPB") durante su primera reunión plenaria tras su creación.

También es relevante tener en cuenta las guías, respuestas, opiniones e informes de la Agencia Española de Protección de Datos ("AEPD"), en particular el informe 164/2018 sobre la incompatibilidad entre DPD y responsable de seguridad.

Sea todo ello en principio como referencia, volveremos sobre las mismas a lo largo del presente Libro Blanco.

Si todo lo anterior define el marco de actuación del DPD y si nos centramos en el objeto de supervisión normativa esta incluye como no puede ser de otra manera el RGPD y otras disposiciones de protección de datos de la Unión Europea y de los Estados Miembros, incluyendo asimismo cuanta normativa interna disponga el responsable o el encargado del tratamiento en relación con esta materia.

Así pues, compondrá el marco normativo de cumplimiento de la actividad diaria de un DPD, como no, el RGPD y la LOPDGDD, la Ley de Servicios de la Sociedad de la Información ("LSSI") y la Ley General de Telecomunicaciones ("LGT2") en lo que respecta a la transposición por ambas normas de la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva "e-Privacy") que actualmente se encuentra en proceso de revisión y actualización en forma de reglamento comunitario.

Es también conveniente incluir en este marco, la Directiva 2016/1148 Del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, (Directiva NIS) dado su impacto en algunos sectores a la hora de identificar e implementar medidas técnicas y organizativas que se puedan considerar apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Es relevante referirse igualmente a los dictámenes, opiniones y guías del mencionado GT29 y su sucesor, el EDPB y cómo no, a las guías, opiniones, informes y resoluciones de la AEPD y Autoridades de protección de datos autonómicas y a los criterios de órganos jurisdiccionales, sin olvidar las implicaciones desde el punto de vista de protección de datos de la muy diversa legislación sectorial.

Por último, por no hablar únicamente del marco normativo en protección de datos, sería de utilidad referirse, al menos brevemente, al aspecto normalizado y estandarizado del mismo. Así, la actividad de la Organización Internacional de Normalización ("ISO") que, por ejemplo en su ISO/IEC 29134:2017 proporciona un estándar en lo relativo al proceso de análisis del impacto en la privacidad, así como la estructura y contenido al documento destinado a recogerlo.

También debe estar presente, en términos de seguridad, los informes y estudios de la Agencia Europea de Seguridad de las Redes y de la Información ("ENISA"), las guías e informes del CCN-CERT o las guías del INCIBE, por citar entre algunos de los posibles y numerosos recursos.

II LA FUNCIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS

II.1.- Designación del delegado de protección de datos.

El artículo 37.1 del RGPD establece tres criterios para los que se considera obligatoria la designación de un DPD:

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

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

- Cuando 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 del RGPD y de datos relativos a condenas e infracciones penales a las que se refiere el artículo 10 del RGPD.

Las mencionadas Directrices del GT29 introducen aclaraciones sobre diferentes aspectos o conceptos de estos criterios. En particular,

- 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.

- A la hora de considerar que significa "observación habitual y sistemática", interpreta "habitual" 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

  y define "sistemático" aquello que se produce de acuerdo con un sistema o que está ejecutado de forma preestablecida, organizada o metódica.

  Sin perjuicio de lo establecido en el mencionado artículo 37 del RGPD, la LOPDGDD en su artículo 34 realiza una enumeración detallada de entidades que están obligadas a designar un DPD. Sin otro afán 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 DPD. En todo caso, la LOPDGDD se refiere a la posible designación voluntaria del DPD que en muchos casos puede ser recomendable, al menos por las siguientes razones:

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

— La Intervención del DPD 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 DPD 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.

II.2. - Realidad del DPD en las organizaciones.

La figura del DPD dentro de las organizaciones españolas ha adquirido especial relevancia desde la plena entrada en vigor del RGPD, pero es necesaria mayor concienciación de las empresas para definir e implantar dicha función.

Las redacción del RGPD provocan dudas acerca de cómo debe ser la posición del DPD y cómo las empresas están implementando esta figura.

Una de las principales cuestiones es el propio **perfil** del DPD. Desde algunos ámbitos se considera que esta figura debe estar subsumida en un perfil jurídico puesto que se trataría de un profesional capaz de interpretar las leyes y las directrices, además de tomar decisiones que no sean contrarias a la normativa vigente. Otros señalan que el DPD no necesariamente tiene que tener perfil jurídico, pero sí que tenga amplios conocimientos jurídicos, técnicos y empresariales.

Existen otras dudas respecto a la posición del DPD, como la **relación** que ha de tener con su organización. La normativa establece que el DPD puede formar parte del personal de la empresa o ser contratado mediante un contrato de servicios. Tal y como establece el GT29, este tipo de profesional puede ser externo,

sobre la base de un contrato de servicios celebrado con una persona física o jurídica. Cuando esta función sea ejercida por un proveedor de servicios externo, esta labor podrá ser ejercida por un equipo de personas bajo la responsabilidad de un contrato y la dirección de un responsable del cliente. En este tipo de contratos es fundamental que se asignen claramente las responsabilidades y tareas dentro del equipo de DPD externo y que se designe a una única persona como contacto principal.

Respecto a las empresas que forman parte de un grupo societario, es interesante referirse a la opinión del GT29 respecto a la posibilidad de si pueden nombrar un **DPD conjunto**. Un grupo de empresas podrá designar un único DPD para el grupo siempre que sea "fácilmente accesible desde cualquier establecimiento". Esto incluye **"la accesibilidad física para el propio personal del grupo y también la posibilidad de que los interesados contacten con el DPD en su lengua"**. Esta accesibilidad se refiere a las tareas del DPD como punto de contacto con el resto de interesados, la autoridad de control y, también, internamente dentro de la organización. Para asegurar esta disponibilidad del DPD, sus datos de contacto deben estar totalmente disponibles y debe estar en condiciones de comunicarse eficazmente, tanto con interesados como con la AEPD. Esta única figura también es extrapolable a autoridades públicas que, teniendo en cuenta su estructura y tamaño, un único DPD pueda ejercer sus funciones. En todo caso, la organización deberá garantizar que ese único DPD pueda llevar a cabo de manera eficaz sus tareas a pesar de haber sido designado para varias autoridades y organismos públicos.

Otro aspecto del DPD que merece ser señalado es su eventual (in)**compatibilidad** con otras figuras encargadas de la seguridad. La normativa establece que el DPO podrá realizar otras funciones siempre y cuando no produzcan un conflicto de interés.

Los requisitos de la normativa establecen que el DPD no podrá ser influenciado por imperativos de negocio, afectando su independencia si se trata de una figura que se dedica a determinar los fines y medios de los tratamientos (por ejemplo, el director de marketing o el director general).

El GT29 señala que la ausencia de conflicto de intereses está estrechamente ligada al requisito de actuar de manera independiente. Aunque los DPD puedan tener otras funciones, solamente se les podrá confiar otras tareas y cometidos si estas no dan lugar a conflictos de intereses. Esto supone, en especial, que el DPD no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso.

Podemos afirmar que la realidad "organizativa" de la figura del DPD en las empresas españolas es muy diferente entre ellas. Cada organización tiene libertad para organizar el DPD y la forma de su designación. Esta figura puede ser un perfil legal o un perfil técnico con conocimientos legales; un DPD interno o externo; una persona individual o un equipo de personas; un DPD para una única sociedad o un DPD para un grupo de sociedades; la concurrencia en la figura del responsable de seguridad o la designación de profesionales separados, etc. Aunque exista libertad en la designación de la figura, el responsable sí que debe cumplir con los requisitos legales, en especial: la independencia, la eficaz realización de sus funciones y, finalmente la ausencia de conflicto de intereses.

III MODELOS ORGANIZATIVOS Y RELACIONALES

III.1. INTRODUCCIÓN.

Ante la ausencia de una previsión normativa específica, las organizaciones han optado por Modelos Organizativos y Relacionales en cuanto al DPD muy diferentes, y basado en criterios también propios y diferentes, como se puede observar en los resultados del ***Primer Estudio sobre el Nivel de Madurez y Cumplimiento del RGPD en España***.

El Modelo Organizativo y Relacional en cuanto a la posición del DPD dentro de la organización tiene un gran impacto, pues de él dependerá en buena parte que este pueda cumplir con sus funciones de forma adecuada y atendiendo a los requisitos que el propio Reglamento marca en su artículo 38:

- Participando en tiempo y forma en todas las cuestiones relativas a Protección de Datos
- Con recursos suficientes y acceso a los datos personales y a las operaciones de tratamiento
- Con independencia
- Sin conflicto de intereses
- Rindiendo cuentas al más alto nivel jerárquico de la organización

En el presente apartado vamos a revisar aquellos modelos más habituales en cuanto a:

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

III.2. DPD EXTERNO, INTERNO O DEPARTAMENTAL.

III.2.1. DPD 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. Opción residual según lo observado en el Estudio sobre el Nivel de Madurez y Cumplimiento RGPD en España, con un 3% de casos.

Según las Directrices sobre los Delegados de Protección de Datos del GT29 esta opción permite que las tareas de DPD contratadas se presten por parte de un equipo del proveedor, pero en este caso todos 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 DPD.

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 DPD 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 DPD accederá como encargado a información personal Responsabilidad del Cliente.

La decisión o no de optar por contratar un servicio externo de DPD depende en gran medida de la estrategia en cuanto al gobierno del dato y de la gestión de la privacidad que se defina en la compañía, de su tamaño y capacidad para dotarse internamente de una persona con el perfil adecuado para asumir el puesto.

Probablemente este modelo no sea el más idóneo para grandes organizaciones, con capacidad para dotarse de áreas de Protección de Datos y de un DPD adecuadamente formado, porque 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 que en organizaciones con tratamientos numerosos, variados y cambiantes de datos personales puede ser un requisito imprescindible. En cambio, en organizaciones más pequeñas podría ser oportuna esta externalización, ante la imposibilidad de dotarse de un DPD adecuado de forma interna.

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 pérdida de independencia

III.2.2. Equipo Departamental.

Según se observa en la encuesta anteriormente citada un importante porcentaje de organizaciones han optado por crear equipos de trabajo que asumirán las funciones del Delegado de Protección de Datos, con un 12% de casos.

Si bien no aparece ni en el Reglamento ni en la LOPDGDD indicación clara en contra de que un órgano multipersonal pueda ser nombrado como Delegado de Protección de datos, y la propia AEPD incluye en su Guía para Comunicar el DPD indicaciones de como comunicar como tal un órgano colegiado o grupo de trabajo, se plantean dudas razonables en este ámbito. La propia redacción de la legislación parece estar pensando en una persona física y no en un órgano multipersonal, especialmente si se tiene en cuenta que se establece específicamente para el caso de DPD externo esta posibilidad. Además, las Directrices del GT29 a la hora de dar indicaciones para casos de grupos de trabajo se refiere a ellos solo para DPD 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 DPD 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 DPD.
- 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 basa en el trabajo transversal dentro de la organización, y puede tener grandes ventajas en aquellas con madurez en este modo de organización, siempre y cuando se hallen realmente representadas las áreas adecuadas. Es un modelo basado en la extensión a la privacidad del modelo interdepartamental de la gestión de la seguridad en base a Comités o Comisiones con atribuciones operativas que venían existiendo ya 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 DPD.

CONTRAS

- Ciertas funciones del DPD 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.

III.2.3. DPD interno.

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

Seguidamente vamos a repasar los modelos organizativos más comunes a la hora de la posición del DPD interno dentro de las empresas privadas.

III.3. MODELO ORGANIZATIVO.

III.3.1. Modelo I: DPD y CISO.

Partiendo del modelo previo al RGPD en el que no existía en España ninguna figura semejante al DPD, pero sí la obligación de nombra un Responsable de Seguridad, muchas empresas podrían optar por asignar el nuevo rol al CISO.

Obviando que la propia figura del Responsable de Seguridad tiene modelos organizativos y de reporte diferentes, nos vamos a centrar en las cuestiones específicas de asignar también a éste las funciones y responsabilidades del DPD. Quizás el tema más importante a tener en cuenta a la hora de asignar ambas responsabilidades es el de qué tipo de CISO existe en la organización, puesto que si bien podría no haber conflicto de intereses con modelos dónde el CISO se centre en el Gobierno de la Seguridad, si podría darse el caso para modelos en los que sus tareas se centren en la primera línea de defensa, con tareas más operativas.

Otra cuestión importante a tener en cuenta es dónde se ubican los riesgos mayores en cuanto a protección de datos en la organización: en los riesgos tecnológicos y de seguridad, con los que el CISO estará perfectamente alineado, o más con los procesos de negocio. Puesto que es difícil que el CISO pueda estar implicado, salvo que se le doten de nuevas herramientas para ello, en fases iniciales de definición de tratamientos cuando todavía no se ha llegado a la definición tecnológica, el DPD ya debe estar en estas primeras fases implicado, en cuanto a los principios de cumplimiento de licitud y proporcionalidad.

Es especialmente relevante la opinión de la AEPD respecto a la concurrencia en una misma persona de las funciones de responsable de la seguridad y DPD. La autoridad establece que la protección de datos trata de un derecho fundamental, mientras que la seguridad de la información es una obligación más de la organización, que deberá aplicar las medidas necesarias para garantizar un nivel de seguridad adecuado al riesgo.

La AEPD concluye que, "con carácter general, debe existir la necesaria separación entre el delgado de protección de datos regulado en el RGPD y el responsable de seguridad, sin que sus funciones puedan recaer en la misma persona u órgano colegiado. Excepcionalmente, en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar dicha separación, sería admisible la designación como DPD de la persona que ejerciera las funciones de responsable de seguridad, siempre que en la misma concurran los requisitos de formación y capacitación previstos en el RGPD". Además, continúa observando la AEPD "resultaría imprescindible adoptar todas las medidas organizativas, debidamente reflejadas en su Política de seguridad de la información, que garantice la necesaria independencia y la ausencia de conflicto de intereses, por lo que no podría recibir instrucciones respecto al desempeño de sus funciones como DPD, deberá responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. En todo caso, esta circunstancia excepcional, deberá evaluarse caso por caso, y deberá dejarse documentada dicha designación haciendo constar los motivos por lo que la organización no ha podido observar dicha separación de funciones, así como las medidas que garantizan la independencia del DPD": como podrían ser la utilización de direcciones de correo electrónico, presupuestos, recursos y reportes diferenciados e independientes.

Así pues, la AEPD establece el carácter excepcional de la concurrencia de ambas figuras, que deberá ser evaluada caso por caso.

PROS

- Implicación directa en la gestión de los riesgos relativos a ciberseguridad

CONTRAS

- Posible conflicto de intereses

III.3.2. Modelo II: DPD y Compliance.

Por otra parte, un número importante de empresas han visto sinergias entre el puesto de Compliance y el de DPD, puesto que ambos puestos tienen como objetivo asegurar el cumplimiento de normas legales dentro de la empresa.

Este modelo puede permitir al DPD tener la ubicación y reporte a la alta dirección ya establecido al Compliance. y podría ser una solución más adecuada para organizaciones en las que la mayor parte de los riesgos en protección de datos provengan de los procesos de negocio y procedimientos implantados.

Hay que tener en cuenta que la labor del Compliance es la de gestionar los riesgos para la organización relacionados con el cumplimiento legal. Mientras que los riesgos que debe gestionar el DPD se refieren a aquellos para los derechos y libertades de los interesados. Importante que la persona que asuma ambas responsabilidades sea capaz de aplicar adecuadamente los dos diferentes enfoques según el caso.

PROS

- Alineamiento en cuanto a la gestión de riesgos (medidas de control)
- Conocimiento requerido de la organización y de sus procesos de negocio

CONTRAS

- Utilizar modelo conjunto de gestión de riesgos global que no se adapte a los requisitos del RGPD sobre riesgos sobre derechos fundamentales
- Menor relación y conocimiento de los medios técnicos de las actividades del tratamiento
- Alejamiento de las áreas de diseño de productos y servicios, en las fases iniciales

III.3.3. Modelo III: DPD en área Jurídica.

Otra posición muy común es asignar a un miembro del área Jurídica las funciones de Delegado de Protección de Datos, exclusivas o añadidas a otras funciones propias del área. Las sinergias en cuanto al conocimiento legal en materia de protección de datos parecen obvias.

En este caso es muy importante tener en cuenta el posible conflicto de interés que puede surgir en caso de que el DPD directamente o como miembro del área jurídica, deba representar al encargado o responsable ante los Tribunales en cuestiones relativas a la protección del datos. Conflicto que el propio GT29 menciona en sus directrices, aunque sólo para el caso de DPD 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 del mismo.

Otra cuestión importante a tener en cuenta es que normalmente las áreas jurídicas se encuentran más alejadas de las áreas responsables de los medios del tratamiento, principalmente del área de Sistemas. Y en estas organizaciones el DPD deberá dotarse de conocimientos e instrumentos adecuados para salvar este posible problema.

PROS

- Alineamiento en cuanto a la definición de modelos contractuales
- Participación en los análisis iniciales de la toma de decisiones estratégicas de la organización.

CONTRAS

- Posible conflicto de intereses.
- Menor relación y conocimiento de los medios técnicos de las actividades del tratamiento.

III.3.4. Modelo IV: Área independiente.

Independientemente de la ubicación posterior en la jerarquía de la organización, más de un 20% de estas han optado por crear un área nueva de Protección de Datos, en la que se ubica el Delegado de Protección de Datos.

Este Modelo permite realmente definir desde el inicio la posición del DPD 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.

PROS

- Oportunidad de definir funciones y relaciones organizacionales ex novo.
- No existen en principio conflictos de interés.

CONTRAS

- La organización tiene que tener la capacidad de dotarse de un área exclusiva en cuanto a recursos y a capacidades del DPD.

IV.4. Modelo Relacional: Reporte y relación con el resto de la organización.

III.4.1. Reporte del DPD.

El DPD debe cumplir sus funciones "Rindiendo cuentas al más alto nivel jerárquico de la organización. Además, en la LOPDGDD se establece una nueva función del DPD en su artículo 36, "cuando aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección". Sin embargo, en ningún momento se define explícitamente qué órganos se consideran alta dirección exactamente. El GT29 en sus Directrices únicamente cita como ejemplo al Consejo de Administración, refiriéndose al deber de Reportar al más alto nivel de administración de la organización.

En base a estas Directrices, y al contenido de la Ley de Sociedades de Capital y en Reglamento de Registro mercantil, en lo que se refiere a los órganos de administración y dirección como aquellos encargados del gobierno, administración y representación de una sociedad, podemos entender que el más alto

Nivel jerárquico se refiere al Consejo de Administración y a cualquier otro órgano en el que este haya delegado oficialmente funciones de administración y dirección, como puede ser Comisiones del Consejo, Consejero Delegado, o Presidente Ejecutivo.

Independientemente del tipo de DPD, el Modelo Organizativo debe incluir las medidas adecuadas para asegurar que el reporte se hará hacia esa alta dirección, de forma efectiva y real. El nivel de reporte no sólo es importante para cumplir con la obligación de rendición del DPD, sino porque es una herramienta básica para asegurar su independencia real y efectiva, así como la eficacia de sus funciones de asesoramiento y supervisión. Si el DPD no puede reportar directamente, por más independientes que sean sus informes e indicaciones, se corre el riesgo de que lleguen filtrados a los órganos de decisión.

Para ello es necesario que el DPD en persona, sea interno o la persona de contacto del DPD externo, tenga acceso directo y sin intermediarios a los órganos de la alta dirección para los que se haya tomado la decisión de que sean su vía de reporte; sin intermediarios, como puede ser su responsable jerárquico.

Según el **Estudio sobre el Nivel de Madurez y Cumplimiento RGPD en España** estos son las áreas de Reporte más comunes, por orden:

- Comisión de Auditoría y Cumplimiento del consejo.
- Consejero Delegado.
- Dirección Jurídica.
- Comité de Dirección.
- CISO.

Como hemos mencionado anteriormente, más allá de que exista una relación de reporte jerárquico directo con el nivel más alto de la organización como sucede en los dos primeros, lo relevante es que la organización defina mecanismos organizativos que habiliten se reporte.

Cualquier otro punto de reporte, como puede ser Dirección de Operaciones, Financiera, Marketing, Recursos Humanos, a priori no cumple el requisito de alta dirección. Además de que se puede entender que resta independencia al DPD, como indica el GT29 en sus directrices. Aunque en estas se refiere más al conflicto de intereses de dotar de las funciones de DPD a puestos, el mismo conflicto o mayor inclusive puede surgir si es a ellas a la que reporta un DPD, interno o externo.

III.4.2. Relación con otras áreas de la organización.

Sin entrar a analizar cómo debe ser la relación del DPD con la organización u organizaciones para las que haya sido designado, es importante que el Modelo Organizativo del puesto haya tenido en cuenta que este tiene que tener establecidas vías de comunicación claras con las áreas mayormente implicadas en las actividades del tratamiento; incluyendo su participación en aquellos Comités u órganos interdepartamentales que tomen decisiones de alto impacto en este sentido.

Será básico que la organización cuente, al menos, con la estructura y la organización que permita que el DPD:

1) conozca y forme parte de la definición de las estrategias de la compañía, fundamentalmente en lo referido aActividades del Tratamiento: nuevos productos y/o servicios, planes de marketing, reorganizaciones internas en cuanto a funcionales laborales, etc.

2) participe de forma activa en la definición, junto con el área de Sistemas o/y Tecnología, del Plan de Sistemas de Información de la organización, pudiendo de esta manera conocerlo profundamente y asegurar que los requisitos en Protección de Datos se contemplan desde la fase de definición inicial de cualquier sistema de tratamiento de datos. Tal como recomienda la propia AEPD.

3) trabaje conjuntamente con el CISO, tanto en la definición de las medidas de seguridad a establecer en las Actividades del Tratamiento y de gestión operativa de incidentes de seguridad, que pudiesen suponer brechas de seguridad.

4) defina conjuntamente con el Área Jurídica las condiciones de contratación de Encargados del Tratamiento.

5) defina con las áreas financieras los requisitos en cuanto a capacidades de cumplir con la legislación en privacidad de los candidatos a ser proveedores.

Mención aparte, requiere la necesaria alineación con el área de auditoría y control de la organización, Auditoría Interna normalmente o cualquier otra que tenga estas atribuciones. Por una parte es necesario definir claramente qué atribuciones tiene el DPD en cuanto a la Supervisión del Cumplimiento en materia

de protección de Datos y cuales ejercerá funcionalmente el área de Auditoría Interna. Sin olvidar, que el DPD es una función más de la organización que igualmente debe ser auditado y controlado en sus funciones, sin que esto suponga o pueda suponer una pérdida de independencia para él.

III.5. Sector Público.

III.5.1. Obligatoriedad de nombramiento de un DPD en el Sector público.

El RGPD dispone que los responsables y encargados de tratamiento deberán designar un Delegado de Protección de Datos en los supuestos que el RGPD establece, así como en otros casos en que la legislación de los Estados Miembros lo consideren también obligatorio. Entre los supuestos en los que el RGPD determina que habrá de designarse un DPD se encuentra el de que "el tratamiento lo lleve a cabo una autoridad u organismo público", tanto en calidad de responsable como en funciones de encargado de tratamiento (artículo 37.1.a RGPD).

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 a las entidades o instituciones de carácter público.

La primera cuestión que podemos plantear es por lo tanto a quién se refiere la norma europea al hablar de autoridades u organismos públicos, y es que el concepto es lo suficientemente amplio como para poder afectar a todo tipo de entidades pertenecientes al sector público, sin poder restringir la noción solamente a las administraciones públicas y sus entes dependientes.

El RGPD no define cuales sean esas autoridades u organismos públicos, dejando por lo tanto al derecho nacional, la concreción del ámbito subjetivo de aplicación de la norma; únicamente se excluyen en forma expresa los tratamientos efectuados por los tribunales en el ejercicio de su función judicial. Obsérvese en todo caso que esta exclusión es material y no subjetiva, pues solo afecta a una determinada función a desarrollar por los tribunales —la judicial— no por lo tanto a otros tratamientos que pudieran ser realizados por el poder judicial. En consecuencia, el poder judicial (Consejo General del Poder Judicial) está incluido en el ámbito de aplicación del artículo 37 pues es autoridad y organismo público.

Para la determinación del concepto de autoridad pública a los efectos de protección de datos en nuestro derecho interno, podríamos también acudir al elenco recogido en el artículo 77 LOPD, pero no parece que esta extrapolación nos

proporcione ni un elenco de autoridades y organismos públicos— ni que el mismo sea completo.

Según el GP29 dentro del concepto de autoridad u organismo público, indudablemente se deben incluir las autoridades nacionales, regionales y locales, lo que trasladado a nuestro derecho, deberá entenderse referido al sector público estatal, autonómico y local. En este sentido, se incluirán, tanto las administraciones públicas propiamente dichas, como claramente los organismos públicos de ellas dependientes y otras instituciones que no son propiamente administración, como las Cortes Generales y sus órganos dependientes (Defensor del Pueblo y Tribunal de Cuentas) y sus órganos análogos en el ámbito autonómico, parlamentos autonómicos y órganos análogos en el caso de que existieran.

Por otra parte, siguiendo en este sentido también las directrices de interpretación del GT29, debe tenerse en cuenta que la labor pública puede llevarse a cabo por organizaciones privadas, lo que refiere no solamente a entidades privadas dependientes de las autoridades públicas (fundaciones públicas, sociedades públicas..) que realicen una labor pública, sino también a personas físicas o jurídicas privadas que realicen esa misma labor (por ejemplo, empresas con contratos de concesión o de servicios…) en tales casos, siguiendo al GT29, los interesados pueden estar "en la misma situación que se produce cuando una organización o autoridad pública trata sus datos", por lo que se entiende que, aun cuando no exista obligación deberá recomendarse como buena práctica de estas organizaciones privadas la designación de un DPD.

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. Podemos, no obstante, perfilar diversos aspectos que, con la necesaria adaptación al supuesto concreto, necesariamente, deberán ser tenidos en cuenta.

III.5.2. DPD 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 RGPD admite la posibilidad de externalización de la figura del DPD. El caso de externalización el DPD 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 autoridades y 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 DPD (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.

III.5.5. Órgano colegiado.

En el caso de que se opte por asumir la tarea con medios propios, es posible la designación de un único DPD 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 (así expresamente se pronuncia el GT29 en su análisis del DPD).

Nada obsta para que la función de DPD sea asumida por un órgano colegiado. Estos órganos colegiados tienen como regulación básica para el caso de la mayor parte de las entidades públicas la recogida en la Ley 40/2015, de Régimen Jurídico del Sector Público (artículo 15 a 24). 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 de Seguridad de las TIC CCN-STIC 801 sobre Esquema Nacional de Seguridad Responsabilidades y Funciones, establece que en 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 del tratamiento".

De 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.

Ejemplo de lo anterior, es la Política de Seguridad de la Información aprobada por la Orden INT/424/2019, de 10 de abril, del Ministerio del Interior, que prevé la existencia de un Comité Superior para la Seguridad de la Información, del que formará parte un representante del Grupo de Trabajo de los Delegados de Protección de Datos, constituido a su vez por los DPDs de las distintas Direcciones Generales.

III.5.6. Modelo organizativo.

En el ámbito del sector público coexisten diversos esquemas organizacionales. Si tenemos en cuenta que el DPD, por sus funciones legalmente determinadas, en parte realiza lo que se denomina "la actividad técnica de la administración", con atribuciones que tienen tanto relevancia interna como externa y que, por otra parte, tiene competencias para producir actos con relevancia jurídica interna y externa, llegamos a la conclusión de que el DPD en las organizaciones públicas debe integrarse en calidad de órgano. Esta calificación es importante, porque supone reconocer al DPD como centro de competencias y atribuciones en materia de protección de datos de la entidad pública correspondiente.

El reconocimiento de la posición del DPD como órgano administrativo implica su capacidad para producir actos con relevancia jurídica y es esencial a la hora de fijar su ubicación orgánica. Esta configuración como órgano en el ámbito de público y en mayor medida en el administrativo, es esencial para garantizar los mínimos de independencia y funcionalidad del DPD. Si, como se expresa en el artículo 38 RGPD y artículo 36 LOPD se deben garantizar al DPD "los recursos necesarios para el desempeño de sus funciones, facilitando los recursos necesarios para su desempeño" y garantizando que "no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones".

La posición del DPD como órgano garantiza tanto su adecuada asignación presupuestaria como su independencia funcional. Ambos aspectos deben considerarse necesarios (dotación de recursos e independencia) pues en caso contrario el nombramiento de un DPD en la organización pública no dejará de ser un acto formal de cumplimiento de una norma inapto para lograr la finalidad de la norma que exige la existencia del DPD en las autoridades e instituciones públicas.

En el órgano puede haber una o varias posiciones o puestos de trabajo dependientes de una jefatura común. En este sentido, por aplicación del principio de autonomía organizativa de las administraciones y entidades públicas, cada entidad deberá en el marco de sus competencia de autoorganización asignar un lugar adecuado al DPD dentro de su estructura que permita con la mayor eficacia obtener el servicio efectivo a los ciudadanos derivado de la regulación en materia de protección de datos personales.

En este aspecto organizativo, son de singular relevancia los principios de jerarquía, descentralización y coordinación, por ello, dadas las funciones del DPD, su adscripción dentro de la estructura de la organización debería hacerse a órganos con competencias y funciones de carácter horizontal, pero con posibilidad de relación directa con la dirección del organismo en el que desempeñe sus funciones. Por ello el concreto puesto de trabajo de DPD, además de tener un perfil, al que luego aludiremos, que sea adecuado para garantizar su reporte al más alto nivel, su inamovilidad e independencia.

Asimismo, el nivel del puesto de trabajo debe ser el adecuado para poder relacionarse con la dirección del órgano u organismo en el que desempeñe sus funciones. Si es interno puede estar dedicado a tiempo completo a las tareas propias del DPD o a tiempo parcial y en ambos casos podría estar respaldado por una unidad específicamente dedicada a la protección de datos, dependiendo de la magnitud y funciones de la entidad.

En cualquier caso, el DPD actúa como asesor y supervisor interno, por lo que ese puesto no puede ser ocupado por unidades o 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 TIC, o responsables de seguridad de la información). (Fuente: Grupo de Trabajo del Artículo 29 en su análisis del DPD); cuestión diferente es que el DPD necesite el apoyo técnico de las unidades implicadas en el tratamiento y seguridad de datos, e incluso la posibilidad de integrar dentro del órgano puestos de trabajo ocupados por personas capacitadas en cuestiones de tratamiento y seguridad

de la información, todo ello dependiendo de la importancia cuantitativa y cualitativa que el tratamiento de datos personales pueda tener en la entidad pública.

III.6. Recomendaciones.

Es importante tener en cuenta a la hora de definir el Modelo Organizativo en cuanto a la figura del Delegado de Protección de Datos de cualquier organización, que no existe un modelo único y que este dependerá en gran medida de las características de esta:

•Tamaño y complejidad organizativa de la empresa
•Factor humano en la alta dirección
•Tipo de Actividades del Tratamiento llevadas a cabo por la organización
•Preponderancia en sus actividades de las nuevas tecnologías y de la innovación
•Ubicaciones geográficas y transfronterizas
•Dicho esto, cualquier modelo organizativo en cuando al DPD puede ser válido, siempre y cuando permita que a través y desde él el DPD pueda:

1. Ser independiente
2. Alinearse con las estrategias, en cuanto al uso de datos personales, de la organización
3. Reportar al más alto nivel de la compañía

Para ello se recomienda que la organización tenga en cuenta sus necesidades y capacidades para optar por el modelo que mejor se ajuste a ella. Y una vez lo tenga especifique claramente dentro de sus procedimientos organizativos, preferiblemente a través de Régimen Interno del DPD o del contrato de prestación de servicios en caso de ser externo, las cuestiones más importantes del Modelo Organizativo y Relacional del DPD:

•Tipo de DPD
•Ubicación y posición 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

IV GOBIERNO DE LA PRIVACIDAD

El Reglamento General de Protección de Datos define como ´Responsable´ y ´Encargado´ del tratamiento de datos personales de las personas físicas, sujetos a esta norma, la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento o los trate por cuenta del responsable, respectivamente.

Son por tanto dichas entidades las obligadas a aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento (artículo 24.1).

Aunque resulta evidente que el RGPD determina que el cumplimiento de las normas sobre protección de datos es responsabilidad corporativa del responsable o encargado del tratamiento, no es menos cierto que a un año de la aplicación de esta nueva norma todavía se mantiene cierta confusión con las funciones del Delegado de Protección de Datos.

El Gobierno Corporativo, como expresión del más alto nivel de las organizaciones, se puede definir como el conjunto de normas, principios y procedimientos que regulan la estructura y el funcionamiento de los órganos de gobierno de las entidades privadas y públicas, en un sentido amplio del concepto, y que estipulan las reglas por las que se rige el proceso de toma de decisiones y asunción de responsabilidades sobre la compañía.

Para el cumplimiento del RGPD, las entidades públicas y privadas deberán establecer las políticas y procedimientos adecuados para garantizar que tanto la entidad, como sus directivos, empleados y terceros cumplen con el marco normativo aplicable.

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

El Gobierno de la Protección de Datos deberá 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;

k) Mantener adecuada información documentada como evidencia de su cumplimiento;

l) Asegurarse de que los encargos de tratamiento con terceros cumplen con la normativa;

m) Promover la mejora continua, realizando el examen de la gestión por lo menos una vez al año;

n) Implementar un programa de auditoría interna para determinar si el sistema de gestión alcanza los objetivos definidos de la organización, se mantiene compatible con la norma, así con los requisitos internos, legales, reglamentarios y contractuales y se mantenga actualizado de manera eficiente;

o) Adoptar las medidas técnicas y organizativas necesarias para disminuir los riesgos de brechas de seguridad y hacer frente a sus consecuencias si no se hubieren podido evitar;

p) Adhesión a códigos de conducta o mecanismos de certificación contemplados en el RGPD, como elementos para demostrar el cumplimiento de sus obligaciones;

q) Articular la rendición de cuentas a la alta dirección, de forma periódica y formal;

IV.2. Modelo de Gobierno de la Protección de Datos.

El Reglamento de Protección de Datos no entra a regular, ni siquiera a recomendar, sobre la forma en que las entidades públicas y privadas deban o puedan articular su gobierno de la protección de datos, más allá de las referencias a la implicación de la "Alta Dirección" o "Alto Nivel Jerárquico" de los responsables o encargados, distribuidas por toda la norma.

Habrá entendido que es más que suficiente con la creación de una nueva figura, obligatoria bajo determinadas premisas, como es la del Delegado de Protección de Datos, dejando a las organizaciones, públicas y privadas, la elección de su modelo de gobierno de la protección de datos, dentro de su libertad de organización o de su esquema de la función pública, que podrá diferir de una organización a otra y vendrá determinado por:

- El tamaño de la organización y el tipo de actividades, procesos, productos y servicios.
- Local, europea o multinacional.
- La complejidad de los procesos y sus interacciones; y
- La competencia de las personas.

A continuación, se muestra un modelo de gobierno de protección de datos que las organizaciones pueden considerar en su estructura de gobierno:

IV.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 que demuestre el compromiso y liderazgo por parte de la alta dirección de la organización. Las políticas son normalmente documentos clave, de alto nivel que deben traducirse posteriormente en procedimientos, estándares y guías que ayuden al cumplimiento de dichos objetivos.

Sin intención de presentar un detalle exhaustivo, a continuación se recogen algunos puntos que pueden formar parte de dicha política:

- Transparencia – Compromiso de proporcionar información clara y suficiente a los interesados sobre el uso de sus datos personales y por parte de quién. En el caso de recoger datos personales de menores u otros colectivos especiales, ajustar el contenido de la información a presentar para que sea entendible.

- Minimización – Compromiso de tratar únicamente la información estrictamente adecuada, pertinente y no excesiva para las finalidades legítimas de la organización y el cumplimiento de obligaciones legales.

- Legitimación – Compromiso de tratar los datos personales de manera leal y lícita, siempre con una base legal adecuada (consentimiento, necesario para la ejecución de un contrato, obligación legal aplicable, proteger intereses vitales del interesado, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos o la satisfacción de intereses legítimos perseguidos) según el tipo de tratamiento.

- Exactitud – Compromiso de establecer mecanismos para mantener la información actualizada y puesta al día cuando sea posible.

- Inventario de Actividades de Procesamiento – Compromiso de crear y mantener actualizado un inventario de actividades de procesamiento de datos personales por la organización, tanto como Responsable de Tratamiento, como Encargado del Tratamiento.

- Retención – Compromiso de mantener la información únicamente mientras sea necesaria por motivos legales, contractuales o por interés legítimo de la organización.

- Derechos de los Interesados – Compromiso de respetar los derechos de los interesados y tomar acción rápidamente para completar el ejercicio de sus derechos y otras cuestiones relacionadas con el tratamiento de sus datos.

- Seguridad de los Datos – Compromiso de tratar los datos de manera segura.

- Transferencias Internacionales – Compromiso de únicamente proceder a la transferencia internacional de datos fuera de la UE con las garantías adecuadas establecidas en las regulaciones y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

- Identificación de Partes Interesadas – Compromiso de identificar las partes internas y externas interesadas en el cumplimiento por parte de la organización, así como el grado de impacto en estructura de Gobierno diseñada por la organización.

- Roles y Responsabilidades Internas – Identificación de los principales roles con responsabilidades internas en el sistema de gestión.

- Revisiones y Auditorías – Compromiso de realización de auditorías internas del sistema de gestión y revisión de la eficacia y eficiencia del mismo por parte de la dirección.

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. 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.

IV.4. Nivel Organizativo – Roles y Relaciones.

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

— 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.

— Delegado de Protección de Datos: El Delegado de Protección de Datos es el enlace entre la alta dirección y el sistema de gestión de protección de datos. A nivel de gobierno, si bien su ruta de escalado suele ser la alta dirección, debe comunicarse y coordinarse con todas las partes interesadas de las diferentes Áreas de Negocio.

— Equipo del Delegado de Protección de Datos: según el tamaño de la organización y la asignación del rol de Delegado de Protección de Datos, es frecuente que este disponga de un equipo de soporte para el desempeño de sus funciones.

— 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.

— 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.

— 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:

- Consejo de Administración: El Delegado de Protección de Datos debe reportar los problemas clave relacionados con el riesgo a la Alta Dirección. Reportar al Consejo de Administración u otro órgano o comité de dirección es lo habitual.

- 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:

    - o Comités Globales: Cumplimiento, Seguridad de la Información, Legal, Ciberseguridad, etc.
    - o País.
    - o Funciones de Negocio.

- 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 con diferentes puntos de enlace con unidades de negocio o responsables de protección de datos por País.

Modelo de Gobierno de Privacidad – Multinacional

IV.5. Problemas prácticos del Gobierno de la Protección de Datos

Podemos decir que la articulación del Gobierno de la Protección de Datos dentro de las organizaciones, tanto públicas como privadas, comparten problemas con los otros ámbitos de cumplimiento, entre otros: el encaje de la figura del Delegado de Protección de Datos, como con el Compliance Officer o con el CISO, en la estructura orgánica de la empresa; líneas de reporting poco claras; estructuras jerárquicas irregulares; órganos de gobierno disfuncionales; poca asignación de presupuesto a la función del DPD, etc.

Entre las obligaciones de los Delegados de Protección de Datos, sino la primordial, está la de hacer llegar la cultura de la protección de datos a todos los miembros de la organización. Para ello, resulta fundamental el apoyo e implicación de la alta dirección, a través del modelo elegido para su Gobierno de la Protección de Datos, en el 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 dentro de una organización 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.

A todo esto, le podemos sumar la falta de cultura de cumplimiento legal de la protección de datos que todavía le cuesta asumir a la dirección de las entidades públicas y privadas, de forma que los directivos de las empresas o de los organismos públicos suelen ver al Delegado de Protección de Datos como alguien que les ralentiza su trabajo, mera burocracia, y no añade valor a la organización.

En consecuencia, este es el reto al que se tienen que enfrentar 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, deberán alcanzar dos objetivos: el primero, 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 el segundo, 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.

V MECANISMOS DE INDEPENDENCIA

Cuando se habla de la figura del DPD y de las cualidades y requisitos que deben tenerse en consideración de cara a su nombramiento, uno de los aspectos que siempre se mencionan y en los que se incide es precisamente en la necesaria Independencia que debe tener.

Esto es especialmente significativo teniendo en cuenta que el RGPD establece la posibilidad de que el DPD pueda desempeñar otro tipo de funciones siempre y cuando se garantice esta "independencia". De este modo, en el artículo 38.6 se establece lo siguiente:

"El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos ***no den lugar a conflicto de intereses****"*.

Este concepto de independencia que puede parecer sencillo, ha generado y genera más de una duda y debate en las organizaciones sobre todo pensando en el nombramiento y selección del DPD. Así pues, se hace necesario profundizar en este concepto, así como identificar específicamente con qué mecanismos puede contar una organización para garantizar precisamente dicha independencia.

Lo primero que hay que tener en cuenta es que, aunque comúnmente se hable de independencia y se dé por supuesto que es un término que aparece en el RGPD, es significativo que el único sitio donde expresamente aparece vinculado a la figura del DPD es en el artículo 36.2 LOPDGDD cuando indica que:

"Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. ***Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses."***

Mientras que en los artículos donde se trata específicamente la figura del DPD no se menciona este aspecto, aunque pudiera deducirse de lo indicado precisamente en el artículo 38.3:

"El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos ***no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones****."*

De igual modo, y de manera previa a la propia LOPDGDD el propio GT29 , con el objetivo de resolver estas dudas, en el documento que elaboró sobre "Directrices sobre los delegados de protección de datos (DPD)" trataba específicamente estos aspectos tanto en el epígrafe 3.3 como en el 3.5.

En el mismo, aparte de lo indicado relativo a la normativa, se incide precisamente en la necesidad de que al DPD no se le instruya sobre cómo abordar un asunto, por ejemplo qué resultado debería lograrse, cómo investigar una queja o si se debe consultar a la autoridad de control,... entendiendo este aspecto como la importancia de que, a la hora de establecer los procedimientos y gestionar los distintos aspectos relacionados con la privacidad y protección de datos, no se tengan en consideración aspectos que nada tengan que ver con la privacidad y la protección de datos.

Esto es importante ya que en ningún caso, significa que no pueda establecerse dentro de la Organización un Marco de Gobierno, y/o Control o un Sistema de Gestión relacionado con la privacidad y protección de datos, que sea de obligado cumplimiento para toda la compañía y, en particular, por la estructura de DPD (en el caso de que exista) sino que para el desarrollo de dicho marco, el DPD Corporativo, que deberá definir el mismo, no se vea condicionado ni sea instruido por el resto de áreas de la Organización o aspectos externos.

Por otra parte, y en relación al conflicto de intereses, se incide precisamente en que este aspecto está estrechamente relacionado con el requisito de actuar de manera independiente y por lo tanto, aunque los DPD puedan tener otras fun-

ciones, solamente podrán confiárseles otras tareas y cometidos si éstas no dan lugar a conflictos de intereses, siendo necesario analizar caso por caso.

De cara a ese análisis y teniendo en cuenta que la figura del DPD es una figura que ya aparecía en la normativa alemana previo a la entrada en vigor del RGPD, puede servir de referencia la sanción que, en el 2016, la Autoridad de Protección de Datos de Baviera impuso a una organización, por no haber atendido la petición que se le había realizado de que nombrase a un DPD diferente, por considerar que existía conflictos de intereses al ser ocupado el cargo por el propio Director de Sistemas. La sentencia consideraba que el DPD actuaba también como administrador de sistemas, supervisándose a sí mismo y, anulando por lo tanto, la independencia necesaria.

Con todo ello, la distinta normativa dibuja la figura que representa al especialista de la empresa o institución, en materia de privacidad, y a quien le corresponde asesorar y vigilar el cumplimiento en dicha materia por parte de aquella. Ese asesoramiento conlleva una responsabilidad, y para su correcto ejercicio, se deben aunar dos características, conocimiento especializado en dicha materia e independencia.

Así, el DPD es independiente en el ejercicio de su función, es decir, en la formulación de sus dictámenes o asesoramientos, pues asume una responsabilidad indelegable asociada a los mismos. Esa independencia no es un atributo exclusivamente exigido por la legislación a los antes citados, sino que es común a un largo número de funcionarios públicos, tales como magistrados, inspectores o técnicos competentes de distintas materias, etc.

Siempre, en todos esos casos citados, independencia y responsabilidad asociada, son las dos caras de una misma moneda. Dado que es él (el funcionario, el auditor, el director de cumplimiento, el DPD, etc.) quien asume las consecuencias de sus "dictámenes", debe ser él mismo de manera responsable, libre y consciente, y no otro, quien decida cuales son estos, pues caso contrario, evidentemente, estaría asumiendo las consecuencias de los actos de otros.

No obstante, ello no significa que tenga que vivir ajeno a la empresa, sino que, posiblemente lo ideal, por el conocimiento de esta que ello le facilita, (no olvidemos que además de asesorar debe supervisar el cumplimiento de los dispuesto en el Reglamento) es que estuviera integrado en la misma, de igual modo que otras funciones claves o de control, definidas en diferentes regulaciones de ori-

gen comunitario, como riesgos, actuariales o auditoría, que también tienen, en su propia definición, el requisito de independencia.

Naturalmente, como se indica anteriormente, esa independencia lo es para esa materia y función concreta, pero no así para la totalidad de su ejercicio o actividad dentro de su organización. Así, lógicamente, estará sujeto a los sistemas y procedimientos de gobierno y de gestión de su organización en los diferentes ámbitos o funciones, así por ejemplo, el DPD de un organismo público, no podrá contratar a quien quiera para incorporarle a su estructura, sino que tendrá que seguir los procedimientos establecidos por la administración para ello, o igualmente tampoco podrá disponer de otro presupuesto que el que se le asigne en los epígrafes correspondientes de la ley de presupuestos generales del estado del año correspondiente, y de igual modo sucederá en las empresas y organizaciones privadas.

La otra cara de esa moneda es que, tal y como se indica en el artículo 38.2 del RGPD será responsabilidad de la organización a la que presta el servicio, facilitarle los recursos necesarios para el desempeño de sus funciones y el acceso a los datos personales y a las operaciones de tratamiento a fin de que le permitan ejercer las misiones y cometidos de forma adecuada, por tanto, poder asumir, consciente y responsablemente, la responsabilidad adecuada.

Esa independencia se puede articular estructuralmente de diversas maneras, pero una obligada e inexcusable, y en la que como se ha dicho, incide el RGPD, es mediante la aplicación del principio de segregación de funciones, por el que debe de estar aislado o separado de aquellas áreas que, lógica y legítimamente, buscan y persiguen el obtener el máximo beneficio para su empresa, a través de la explotación sistemática y masiva de los datos en poder de la misma.

Así, el propio documento del GT29 antes citado, establece como otros cargos en conflicto con el de DPD, el del director de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos, director del departamento de TI u otros cargos inferiores en la estructura organizativa, si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento.

Esa no es una lista cerrada, entre otras, porque las denominaciones y estructuras varían en cada organización y por tanto debe entenderse como un listado de referencia, en el que, por ejemplo, si se redactase en estos momentos, seguro incluiría nuevas áreas, como las ahora denominadas de Data Analitics o Inteligencia artificial.

Al final, lo que debe prevalecer es la separación de funciones entre, quienes deben velar porque en su organización se respeten las limitaciones al tratamiento y los derechos de los interesados, titulares de los mismos, y aquellos que, dentro de la misma, tienen por cometido el definir y lograr el mayor uso de esos datos, en beneficio de la empresa. Con ello se busca lograr, a través de una figura independiente, que es el DPD, un equilibrio de fuerzas que contrapese y controle, el lógico y legítimo apetito de riesgo de quienes captan, tratan y explotan esos datos.

Pero no solo podemos encontrar ese posible conflicto de intereses con quienes tratan los datos, pues sin duda lo habrá con otras áreas de la organización, así, por ejemplo, con aquella área o figura que deba defender y representar a la organización ante los tribunales, dado que esa figura deberá, legítimamente y con independencia de su personal criterio, asumir y defender, la postura y actuación de su empresa. Lo que naturalmente colisionaría, con la necesidad de independencia de criterio del DPD, quien debe asesorar y defender lo que crea adecuado a la legislación y los derechos de los terceros, con independencia de lo que, en un determinado momento sea oportuno o conveniente para su organización.

Más allá de eso, no debe pensarse, a priori y excepto en los casos evidentes o flagrantes que cita el GT29 antes mencionado, en áreas o figuras que pueden o no pueden ser DPD, pues dependerá en mucho de la organización y de la estructura que, en el ejercicio de su potestad organizativa, esta se haya dotado y, sobre todo, de las funciones asignadas a cada área y, por supuesto, de las competencias de las personas que lideran las mismas. No hay dos organizaciones iguales y por lo tanto no se pueden extraer y extrapolar de una a otra, conclusiones directamente sobre la capacidad o no, sin haber realizado el análisis de la situación concreta.

Dicho esto, y en base a lo anterior, sí que parece adecuado tratar de identificar los distintos mecanismos con los que puede contar una Organización a la hora de garantizar esta necesaria independencia del DPD. Entre los distintos mecanismos en los que se podría pensar a la hora de garantizar la independencia, se encontrarían los siguientes, aunque algunos de ellos, en contra de lo que pudiera pensarse en un primer momento, no implican, per sé, ese concepto de independencia:

•Área Independiente:

Entendiendo como tal al área que esté identificada en el organigrama de la compañía, como un área específica de privacidad y protección de datos (aunque esté formada únicamente por el DPD y no cuente con una estructura organizativa).

Aunque este podría considerarse que es uno de los mecanismos que por sí mismo garantizarían esa independencia, pero no debe perderse de vista el necesario cumplimiento del resto de requisitos que deben ser tenidos en consideración de cara al nombramiento del DPD y que hace que no siempre sea posible, ni lo más adecuado, la creación de un área independiente, si la misma no tiene ni la entidad, status y competencias que realmente deba tener el DPD. Además, salvo que tenga una posición que dependa directamente del máximo responsable de la organización (CEO de la empresa, director de un organismo, etc), en general, siempre habrá una dependencia de otra área.

Así pues, incluso en este caso, es necesario garantizar y documentar la existencia de esta independencia, la ausencia de conflictos de intereses y la capacidad y recursos necesarios que la posibiliten.

•DPD Externo:

Este es otro de los mecanismos que identifican muchas organizaciones para garantizar esta independencia pero que, al igual que el caso anterior, tiene que ser analizado en detalle ya que, per se, tampoco conlleva directamente el cumplimiento de todos y cada uno de los requisitos de la organización.

Ante el nombramiento de un DPD Externo siempre habrá un área de la Organización que sea la que mantenga dicho contacto con el DPD y por lo tanto en función de quien sea esa área y la ascendencia y capacidad de presión que tenga sobre esa empresa externa puede condicionar precisamente ese carácter de independencia que necesariamente tiene que tener.

Para ilustrar ese caso, baste con pensar en un área de marketing o de TI, que contraten con su principal proveedor, además de los servicios propios de sus áreas, el de DPD, y que este se lo proporcione en el mismo contrato de prestación y por personal que además, participe en otros servicios.

Así pues, es necesario volver a incidir en la necesidad de analizar el caso concreto, confirmar que se cumplen cada uno de los aspectos requeridos y la necesaria documentación de todo ello.

•Modelos basados en las Tres Líneas de Defensa

El marco de referencia COSO de Control Interno y el modelo de tres líneas de defensa, está implantado, a día de hoy, en muchas organizaciones que, bien por obligación o por convencimiento, lo han adoptado y por tanto cuentan con un

sistema organizativo con estructuras de gobierno y control, divididas en las Tres Líneas de Defensa.

Este modelo distingue tres líneas de actividades (o defensa) que participan en una efectiva gestión y supervisión de riesgos:

- La primera línea compuesta por el control de la gerencia, donde cada área operativa o funcional de la organización, pone en práctica la gestión de sus propios riesgos y controles. Es donde podríamos considerar está ubicado el grueso de la organización y el core de negocio.

- La segunda línea contempla las funciones de supervisión de riesgos, controles y cumplimiento de políticas y estándares establecidas. Donde suelen estar situadas un conjunto no cerrado de figuras y responsables de funciones (Riesgos, Cumplimiento, Actuarial, Seguridad, Control Interno, etc) que tiene entre sus características el conocimiento altamente especializado de la materia que trata, la independencia de la primera línea de defensa, la responsabilidad asociada al ejercicio de su cargo y el reporte a la Alta Dirección.

- La tercera línea compuesta por Auditoria Interna, que aporta, entre otros, supervisión objetiva sobre las dos primeras líneas de defensa y es a la vez, garante último de los intereses de los accionistas y cumplimiento de las leyes.

La ubicación natural y lógica del DPD, en las organizaciones que adopten este modelo de gobierno y control basado en tres líneas, sería en esa 2ª línea de defensa, sin encontrarse incompatibilidades, al menos per se, para que su ejercicio se combine con el de alguna otras actividades, siempre, eso sí, que esas sean también de esa segunda línea, y por tanto compartan las características de independencia de la primera línea, responsabilidad asociada al ejercicio de su cargo y el reporte a la Alta Dirección.

•Comité de Independencia

En determinadas organizaciones que están obligadas a garantizar en todo momento un adecuado control de los conflictos de intereses que pudieran existir en el desempeño de sus funciones (empresas auditoras, consultoras, ...), existen comités específicos de Independencia donde se elevan, analizan las distintas situaciones que pudieran general conflicto de intereses y se garantiza que las mismas no lleguen a producirse.

Estos mismos Comités podrían ampliar su alcance y podrían ser utilizados precisamente para garantizar y controlar la ausencia de conflicto de intereses en el nombramiento del DPD y en el desempeño de sus funciones.

•Comité específico de Privacidad y Protección de Datos

Otro de los mecanismos que puede ser utilizado por las organizaciones de manera análoga a los Comités de Independencia antes citados, es la creación de Comités específicos de Privacidad y Protección de Datos.

Estos Comités tendrían entre sus funciones, el servir de apoyo al DPD y garantizar que, en el diseño y la toma de decisiones en materias de privacidad y protección de datos, no existe conflicto de intereses.

De igual modo, y ante situaciones que pudieran considerarse un conflicto de intereses, estas serían analizadas y documentadas por el propio Comité, estableciéndose los mecanismos y soluciones adoptadas por este para evitar dicho conflicto.

Es necesario señalar la importancia de que, para que este comité sirva de mecanismo de independencia, en el mismo estén representados miembros de otras áreas de la Organización como Cumplimiento, Jurídico, etc.

•Documentación de la Independencia

Este es un mecanismo a utilizar por sí mismo o combinado con alguno de los anteriores. Consiste precisamente en establecer dentro de la organización las propias directrices y procedimientos que garanticen la necesidad de realizar, previo al nombramiento del DPD, un análisis y documentación de las funciones y competencias del DPD y la necesaria verificación de esta independencia y conflicto de intereses.

Así como la necesidad de, una vez nombrado el DPD, analizar y documentar toda aquella situación que pudiera considerarse que conlleva algún tipo de conflicto de interés.

En dicho análisis, deberá quedar reflejada al menos la naturaleza del conflicto, las acciones efectuadas para su análisis, la conclusión sobre su efectiva existencia, así como las soluciones o medidas adoptadas.

VI EL PERFIL DEL DELEGADO DE PROTECCIÓN DE DATOS

Cualificación

El DPD será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar 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 DPD con un profundo conocimiento del Reglamento, del sector y del negocio de la propia organización y del propio modelo de negocio de la organización (en particular, cuando se sustente en el tratamiento de datos personales) para facilita 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 (CEDPD) señala que el hecho de tener conocimientos especializados en derechos 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.

Experiencia Profesional

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

a) Conocimiento en el campo de la normativa de protección de datos

Estarán familiarizados 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.

b) Conocimiento en el ámbito TIC

El DPD debe tener conocimientos técnicos básicos y comprender los problemas relacionados con las tecnologías de la información:

— Organización del entorno TIC.

— Estructuras de sistemas, aplicaciones y procesos informáticos.

— Conocer la arquitectura de sistemas de su organización.

— 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.

c) Conocimientos en la Administración y organización de empresas

El DPD debería tener los siguientes conocimientos, al menos básicos, de administración de empresas y organización para que puedan evaluar los problemas en el contexto de una empresa:

— Gestión de Procesos en empresas.

— Sistemas de gestión.

— Regulaciones y Procedimientos administrativos aplicables.

— Métodos de evaluación de riesgos.

— Procedimientos de auditoría y seguimiento.

Habilidades Personales

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

Este tipo de competencias, algunas innatas otras aprendidas, están relacionadas 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:

- Introspectivas: aprender a gestionar emociones, cambiar creencias limitadoras, identificar fortalezas y puntos de mejora, incrementar la auto-conciencia y el sentido de auto-eficacia.

- 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.

- 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 DPD 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 DPD 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 DPD 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 DPD 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 conlleva per se el hecho de contar o reunir las referidas habilidades, por lo que un DPD puede recaer tanto en un perfil de corte jurídico o de corte técnico.

Formación

Sin duda, resulta elemental la formación continua del DPD 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 DPDs, 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.

Deber de secreto

Según establece en el artículo 38.5.RGPD el DPD, 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.

Perfil del DPD en el sector público

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

Por su parte, el artículo 35 LOPD determina que el DPD 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 DPD 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 DPD 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 DPD; si hemos admitido la posibilidad de que se externalice el DPD mediante un contrato de servicios, parece que entendemos que entre las funciones del DPD no está la del ejercicio de la autoridad. Ahora bien, analizadas las funciones del DPD, pue-

de 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 LOPDGDD, 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 DPD 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 DPD, 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 DPD el que deba instruir o pronunciarse en relación con esa reclamación. No se otorga al DPD competencia en la resolución del asunto: la norma se limita a designar al DPD 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 DPD 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 DPD, podremos hablar de una intervención del DPD 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 DPD son las mismas que las ya comentadas para el DPD en el ámbito privado. La especialidad en este caso se encuentra en las competencias generales exigibles.

El DPD 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 DPD en este ámbito.

Por último, simplemente constatar que, dependiendo de la actividad, podrá pensarse en un DPD 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 DPD.

Más información en:

www.ismsforum.es