ANEXO WP243 - PREGUNTAS MÁS FRECUENTES

El objetivo del presente anexo es responder, en un formato simplificado y de fácil lectura, a algunas de las preguntas clave que las organizaciones pueden plantear con respecto a los nuevos requisitos de designación de un delegado de protección de datos (DPD) en virtud del RGPD.

Designación del DPD (artículo 37)

1 ¿Qué organizaciones deben nombrar un DPD? (artículo 37, apartado 1)

El RGPD exige la designación de un DPD en tres casos concretos:

- cuando el tratamiento lo lleve a cabo una autoridad u organismo público (con independencia del tipo de datos que se traten);
- cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala; o
- cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales o de datos relativos a condenas e infracciones penales.

Téngase en cuenta que el Derecho de la Unión o de los Estados miembros podrá exigir el nombramiento de un DPD también en otras circunstancias. Finalmente, en algunos casos en los que el RGPD no requiere específicamente el nombramiento de un DPD, las organizaciones pueden considerar de utilidad designar un DPD de manera voluntaria. El Grupo de Trabajo sobre protección de datos del artículo 29 alienta estos esfuerzos voluntarios.

Para más información, véase la sección 2.1 de las directrices.

2 ¿Qué significa el concepto de «actividades principales»? [artículo 37, apartado 1, letras b) y c)]

Las «actividades principales» pueden considerarse las operaciones clave necesarias para lograr los objetivos del responsable o del encargado del tratamiento. Dichas actividades incluyen también todas las actividades en las que el tratamiento de datos sea una parte indisoluble de la actividad del responsable o del encargado del tratamiento. Por ejemplo, el tratamiento de datos relativos a la salud, como historiales de pacientes, debe considerarse una de las actividades principales de cualquier hospital y, por ello, los hospitales deben designar un DPD.

Por otra parte, todas las organizaciones llevan a cabo determinadas actividades secundarias, por ejemplo, pagar a sus empleados o realizar actividades ordinarias de apoyo de TI. Dichas actividades son necesarias para la actividad principal o el negocio principal de la organización. Aunque estas actividades son necesarias o esenciales, normalmente se consideran funciones auxiliares y no la actividad principal.

Para más información, véase la sección 2.1.2 de las directrices.

3 ¿Qué significa el concepto de «a gran escala»? [artículo 37, apartado 1, letras b) y c)]

El RGPD no define qué actividades constituyen un tratamiento a gran escala. El Grupo de Trabajo del artículo 29 recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala:

- el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
- el volumen de datos o la variedad de elementos de los datos que son objeto del tratamiento;
- la duración, o permanencia, de la actividad de tratamiento de datos;
- el alcance geográfico de la actividad de tratamiento.

Como ejemplos de tratamiento a gran escala cabe citar:

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

Como casos que no constituyen tratamiento a gran escala cabe señalar:

- el tratamiento de datos de pacientes por parte de un solo médico;
- el tratamiento de datos personales relativos a condenas e infracciones penales por parte de un abogado.

Para más información, véase la sección 2.1.3 de las directrices.

4 ¿Qué significa el concepto de «observación habitual y sistemática»? [artículo 37, apartado 1, letra b)]

El concepto de observación habitual y sistemática de interesados no está definido en el RGPD pero incluye, sin duda, todas las formas de seguimiento y elaboración de perfiles en internet, inclusive con fines de publicidad comportamental. No obstante, el concepto de observación no se limita al entorno de internet.

El Grupo de Trabajo interpreta «habitual» con uno o más de los siguientes significados:

- continuado o que se produce a intervalos concretos durante un periodo concreto;
- recurrente o repetido en momentos prefijados;
- que tiene lugar de forma constante o periódica.

El Grupo de Trabajo interpreta «sistemático» con uno o más de los siguientes significados:

- que se produce de acuerdo con un sistema;
- preestablecido, organizado o metódico;
- que tiene lugar como parte de un plan general de recogida de datos;
- llevado a cabo como parte de una estrategia.

Ejemplos de actividades que pueden constituir una observación habitual y sistemática de interesados son: operar una red de telecomunicaciones; prestar servicios de telecomunicaciones; redirigir correos electrónicos; elaborar perfiles y otorgar puntuación con fines de evaluación de riesgos (p. ej. para determinar la calificación crediticia, establecer primas de seguros, prevenir el fraude, detectar blanqueo de dinero); seguir la ubicación, por ejemplo, mediante aplicaciones móviles; programas de fidelidad; publicidad comportamental; observar los datos de bienestar, estado físico y salud mediante dispositivos ponibles; televisión de circuito cerrado; dispositivos conectados, como medidores inteligentes, coches inteligentes, domótica, etc.

Para más información, véase la sección 2.1.4 de las directrices.

5 ¿Pueden las organizaciones nombrar un DPD de forma conjunta? Si es así, ¿en qué condiciones? (artículo 37, apartados 2 y 3)

El RGPD establece que un grupo empresarial puede designar un único DPD, siempre que este «*sea fácilmente accesible desde cada establecimiento*». La noción de accesibilidad se refiere a las funciones del DPD como punto de contacto con respecto a los interesados, la autoridad de control y la propia organización con carácter interno. Con el fin de garantizar que el DPD, ya sea interno o externo, sea accesible, es importante asegurarse de que se dispone de sus datos de contacto, de conformidad con el RGPD. El DPD debe estar en condiciones de comunicarse eficazmente con los interesados y cooperar con las correspondientes autoridades de control. Esto significa que dicha comunicación debe tener lugar en el idioma o idiomas utilizados por las autoridades de control y los interesados afectados. La disponibilidad personal de un DPD (ya sea físicamente en las mismas instalaciones como empleado, ya sea en línea o mediante otros medios seguros de comunicación) es fundamental para garantizar que los interesados puedan contactar con él.

Para más información, véase la sección 2.3 de las directrices.

6 ¿Es posible nombrar un DPD externo (artículo 37, apartado 6)?

Sí. De conformidad con el artículo 37, apartado 6, el DPD podrá ser un miembro de la plantilla del responsable o del encargado el tratamiento (DPD interno) o «desempeñar sus funciones en el marco de un contrato de servicios». Esto significa que el DPD puede ser externo y, en ese caso, su función puede ejercerse sobre la base de un contrato de servicios suscrito con una persona física o una organización.

Si el DPD es externo, se le aplicarán todos los requisitos de los artículos 37 a 39. Tal y como se establece en las directrices, cuando la función del DPD la ejerza un proveedor de servicios externo, un grupo de personas que trabaje para dicha entidad podrá desarrollar efectivamente las funciones de DPD como equipo, bajo la responsabilidad de un contacto principal designado como persona «a cargo» para el cliente. En ese caso, es fundamental que cada miembro de la organización externa que ejerza las funciones de DPD cumpla todos los requisitos aplicables del RGPD.

En aras de la claridad jurídica y de la buena organización, las directrices recomiendan que el contrato de servicios distribuya de manera clara las tareas dentro del equipo de los DPD externos y que se designe una única persona como contacto principal y persona «a cargo» de cada cliente.

Para más información, véanse las secciones 2.3, 2.4 y 3.5 de las directrices.

7 ¿Cuáles son las cualidades profesionales que debería tener un DPD (artículo 37, apartado 5)?

El RGPD establece 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».

El nivel de conocimientos especializados necesario se debe determinar en función de las operaciones de tratamiento de datos realizadas y de la protección exigida para los datos personales tratados. Por ejemplo, cuando la actividad de tratamiento de los datos sea especialmente compleja, o cuando implique una gran cantidad de datos sensibles, el DPD podría necesitar un nivel mayor de conocimientos y apoyo.

Las competencias y conocimientos necesarios incluyen:

- conocimientos especializados sobre la legislación y prácticas nacionales y europeas en materia de protección de datos y una profunda comprensión del RGPD;
- comprensión de las operaciones de tratamiento que se llevan a cabo;
- comprensión de las tecnologías de la información y de la seguridad de los datos;
- conocimiento del sector empresarial y de la organización;
- capacidad para fomentar una cultura de protección de datos dentro de la organización.

Para más información, véase la sección 2.4 de las directrices.

Posición del DPD (artículo 38)

8 ¿Qué recursos deben proporcionarse al DPD para que lleve a cabo sus funciones?

El artículo 38, apartado 2, del RGPD prevé que la organización respalde a su DPD «facilitando los recursos necesarios para el desempeño de [sus] funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados».

Dependiendo de la naturaleza de las actividades de tratamiento y de la actividad y el tamaño de la organización, se deberán asignar los siguientes recursos al DPD:

- apoyo activo a la labor del DPD por parte de la alta dirección;
- tiempo suficiente para que el DPD cumpla con sus funciones;
- apoyo adecuado en cuanto a recursos financieros, infraestructura (locales, instalaciones, equipos) y personal según se requiera;
- comunicación oficial de la designación del DPD a toda la plantilla;
- acceso a otros servicios dentro de la organización de modo que los DPD puedan recibir apoyo esencial, datos e información de dichos servicios;

- formación continua.

Para más información, véase la sección 3.2 de las directrices.

9 ¿Cuáles son las garantías que permiten al DPD desempeñar sus funciones de manera independiente (artículo 38, apartado 3)?

Existen diversas salvaguardias que permiten al DPD actuar de manera independiente, tal y como se señala en el considerando 97:

- no recibirá instrucciones por parte de los responsables o encargados del tratamiento en lo relativo al desempeño de las funciones del DPD;
- no podrá ser sancionado o destituido por el responsable del tratamiento por el desempeño de sus funciones;
- no habrá conflictos de intereses con otras posibles funciones y obligaciones.

Para más información, véanse las secciones 3.3 a 3.5 de las directrices.

10 ¿Cuáles son las «otras funciones y cometidos» de un DPD que pueden dar lugar a un conflicto de intereses (artículo 38, apartado 6)?

El DPD no puede ocupar un cargo dentro de la organización que le permita determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso.

Como norma general, los cargos en conflicto pueden incluir los puestos de alta dirección (tales como director general, director de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI) pero también otros cargos inferiores en la estructura organizativa si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento.

Para más información, véase la sección 3.5 de las directrices.

Funciones del DPD (artículo 39)

11 ¿Qué conlleva el concepto de «supervisión del cumplimiento» del RGPD [artículo 39, apartado 1, letra b)]?

Como parte de las obligaciones de supervisión del cumplimiento, los DPD pueden, en particular:

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

Para más información, véase la sección 4.1 de las directrices.

12 ¿Es el DPD responsable personalmente del incumplimiento del RGPD?

No, el DPD no es responsable personalmente del incumplimiento del RGPD. El RGPD establece claramente que es el responsable o el encargado del tratamiento quien está obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza de conformidad con sus disposiciones (artículo 24, apartado 1). El cumplimiento de las normas en materia de protección de datos es responsabilidad del responsable o del encargado.

13 ¿Cuál es el papel del DPD con respecto a la evaluación de impacto relativa a la protección de datos [artículo 37, apartado 1, letra c)] y al registro de las actividades de tratamiento (artículo 30)?

En cuanto a la evaluación de impacto relativa a la protección de datos, el responsable o el encargado del tratamiento debe recabar el asesoramiento del DPD sobre, entre otras, las siguientes cuestiones:

- si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos;
- qué metodología debe seguirse para llevar a cabo una evaluación de impacto;
- si debe realizarse la evaluación de impacto en la propia organización o subcontratarse;
- qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los interesados;
- si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con el RGPD.

Para más información, véase la sección 4.2 de las directrices.

En cuanto a los registros de las actividades de tratamiento, es obligación del responsable o del encargado del tratamiento, y no del DPD, mantener los registros de las operaciones de tratamiento. No obstante, nada impide que el responsable o el encargado del tratamiento asigne al DPD la tarea de mantener un registro de las operaciones de tratamiento bajo la responsabilidad del responsable del tratamiento. Dicho registro debe considerarse una de las herramientas que permiten al DPD realizar sus funciones de supervisión del cumplimiento, información y asesoramiento al responsable o al encargado del tratamiento.

Para más información, véase la sección 4.4 de las directrices.