EL ENCAJE EN LAS EMPRESAS DEL «DATA PROTECTION OFFICER»

Daniel LÓPEZ CARBALLO

Socio de ECIJA

Dreamstime

El Reglamento Europeo de Protección de Datos (RGPD) plantea nuevas obligaciones y retos para las empresas en relación al tratamiento de datos personales, que deben ser afrontadas antes de su plena aplicación en mayo de 2018

La entrada en vigor del Reglamento Europeo de Protección de Datos (RGPD) plantea nuevas obligaciones y retos para las empresas en relación al tratamiento de datos personales, que deben ser afrontadas antes de su plena aplicación en mayo de 2018.

Entre estas obligaciones se encuentra la necesidad de contar, en diferentes casos, con la figura de un Data Protection Officer (DPO). Una nueva figura, cuya principal obligación será la observancia del cumplimiento de los aspectos establecidos en el RGPD exigibles a la entidad para la que actúe.

¿Quién debe contar con un DPO?

El RGPD establece diferentes casos en los que se deberá contar con un Data Protection Officer:

–Cuando el tratamiento se realice por una autoridad u organismo público, excepto los tribunales en el desarrollo de su función judicial.

Sobre este aspecto, el Grupo de Trabajo del Artículo 29 (WP29) especifica que aquellos casos en los que hay funciones públicas llevadas a cabo por terceros que no tienen naturaleza pública, pese a no ser obligatoria para éstos a priori, podría ser una buena práctica.

–Cuando la actividad principal consista en el tratamiento que requiera una observación habitual y sistemática de interesados a gran escala.

El WP29 interpreta el término habitual, entre otros casos, cuando éste es recurrente en el tiempo, durante determinados períodos o de forma constante.

–Cuando las actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos o relativos a condenas e infracciones penales.

En este sentido, en relación con el concepto de gran escala, hay que tener en cuenta determinados parámetros, tales como la cantidad de interesados afectados por el tratamiento, el volumen de datos tratados, la duración y extensión geográfica del mismo.

A raíz del Anteproyecto de Ley de Protección de Datos presentado por el Ministerio de Justicia, estos supuestos podrían ampliarse considerablemente. En este sentido, se especifican quince supuestos en los que es obligatorio designar un DPO, entre los cuales se encuentran: Colegios Profesionales y Consejos Generales, entidades que exploten redes y presten servicios de comunicaciones electrónicas, prestadores de servicios de la sociedad de la información que recaben información de sus servicios, entidades aseguradoras y reaseguradoras, entidades que desarrollen actividades de publicidad y prospección comercial y centros sanitarios.

En relación con los encargados del tratamiento, deberán contar con un DPO en caso de cumplir alguno de los requisitos mencionados.

¿Cómo nombrar un DPO?

La normativa permite que un grupo empresarial u organismo público designe un sólo DPO atendiendo a su estructura organizativa y con la condición de que éste sea fácilmente accesible, es decir, que pueda cumplir sus funciones, tanto de contacto con los interesados, como de supervisión en el seno de la organización.

Una vez hayamos definido si nos encontramos obligados a nombrar un DPO o, sin estarlo, deseamos contar con esta figura, debemos tener en cuenta que debe exigirse al DPO un conocimiento especializado en materia de protección de datos, debiendo valorarse el mismo, atendiendo a la sensibilidad, complejidad y cantidad de tratamientos de datos realizados en el seno de la organización, junto con su experiencia y cualidades profesionales.

Debe recordarse que la figura del DPO puede externalizarse siempre y cuando se exija un mayor control y el aseguramiento de que el profesional designado cumple con los requisitos enunciados, tiendo capacidad para llevarlos a cabo.

¿Cómo integramos el DPO en la entidad?

Conforme a la normativa europea, el DPO debe formar parte de todos los debates, análisis o discusiones que tengan como materia, directa o indirectamente, el tratamiento de datos personales en el seno de la organización.

Así las cosas, debe ser una figura independiente y autónoma dentro de la organización, con el apoyo de la alta dirección, debiendo tener recursos y tiempo para afrontar sus funciones, facilitándosele la formación necesaria y definiéndose las políticas de comunicación necesarias para que el personal conozca al DPO, sus funciones y los medios de contacto.

Deberá tener acceso y relación con otras áreas para poder desarrollar sus funciones, no pudiendo ser penalizado por la entidad en el desarrollo de sus funciones, debiendo garantizarse que no reciba ninguna instrucción en relación con las mismas.

¿Qué funciones tendrá el DPO?

Entre las principales funciones que tendrá, conforme a la nueva normativa en materia de protección de datos, pueden destacarse:

- Asegurar el cumplimiento normativo, mediante la recolección de información, su análisis y revisión en relación con los tratamientos de datos llevados a cabo, realizando cuantas recomendaciones fuesen necesarias.
- Informar y asesorar sobre las obligaciones que afectan a la entidad y sus empleados o proveedores.
- Supervisar el cumplimiento de aspectos tales como la asignación de responsabilidades, concienciación y formación del personal, así como las auditorías correspondientes.
- Cooperar con la autoridad de control actuando como punto de contacto con la misma.
- Participar en el desarrollo y ejecución de las evaluaciones de impacto, asesorando sobre la obligatoriedad o idoneidad sobre la realización de un PIA, la definición de la metodología e idoneidad de realizar la evaluación por parte de la entidad, o la definición de las medidas a implementar, entre otras cuestiones.
- Igualmente, el DPO deberá gestionar un registro actualizado de los tratamientos llevados a cabo en el seno de la entidad.

Relevancia y riesgos asociados al incumplimiento.

La adopción de estas medidas supone un reto para las entidades, en relación con el cumplimiento de la nueva normativa y su proceso de adaptación a la misma. Aspectos que adquieren mayor relevancia atendiendo a los riesgos asociados y las nuevas infracciones y sanciones que podrían llegar a los veinte millones de euros o el 4% del volumen de negocio total anual global.