¿QUÉ TIENEN QUE TENER EN CUENTA LOS DESPACHOS DE ABOGADOS ANTE LA ENTRADA EN VIGOR DEL NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS?

Maria Diví. Directora del área de Derecho Digital de Herrero & Asociados

SUMARIO

En mayo de 2016 se aprobó el Reglamento UE 2016/679, el Reglamento General de Protección de Datos de la Unión Europea, muy conocido por sus siglas RGPD (en castellano) o GDPR (en inglés), y que es de aplicación desde el 25 de mayo de este año, fecha en la que quedó derogada la Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa 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 virtud de la aplicación del Reglamento, **nuestra Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal** quedó desfasada y se sustituye por una nueva LO. Actualmente, el Proyecto de Ley se encuentra en fase de cierre de enmiendas y no podemos saber cuándo será aprobada ni cuándo entrará en vigor. De todos modos, el Reglamento es directamente aplicable y para todos los Estados Miembros de la UE, pasa a ser la norma de referencia en la materia.

Las novedades afectan por igual a cualquier tipo de empresas, **si bien es mucho más importante en el caso de firmas de abogados en las que el cumplimiento de la ley ha de ser más escrupuloso.**

El Reglamento Europeo prevé nuevas obligaciones, necesarias para proteger los derechos de los interesados, con las nuevas tecnologías actuales. Esta nueva legislación hace especial hincapié en la **responsabilidad proactiva**, es decir, que las organizaciones hagan un análisis del tipo de datos que trata, las finalidades y qué tratamiento se les da a esos datos con el objetivo de garantizar y demostrar que se cumple con todos los aspectos legales que se les exige. **Todas las empresas, despachos y profesionales autónomos** (que traten o recojan datos de carácter personal) **se ven afectados por el nuevo Reglamento y deben implantar los nuevos principios y obligaciones en materia de privacidad,** por lo que es muy importante que todos conozcamos de primera mano la nueva legislación.

El ámbito de aplicación del GDPR engloba el tratamiento de datos personales por parte de un Responsable

"El GDPR prohíbe el consentimiento tácito o presunto y es obligatorio el consentimiento inequívoco"

LEGISLACIÓN

www.casosreales.es

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. (Legislación. Marginal: 70341505). Arts.; 9, 10, 83
- Directiva 95/46/CE del parlamento europeo y del consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (Legislación. Marginal: 56066)
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (Legislación. Marginal: 105103). Arts.; 25 a 32
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (Legislación. Marginal: 72032)

> **"Todos los responsables deben realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo"**

JURISPRUDENCIA

www.casosreales.es

- Sentencia de Audiencia Nacional de 5 de marzo de 2013, núm. 0/0, Nº Rec. 391/2011, (Marginal: 2423085)
- Sentencia de la Audiencia Nacional de 4 de febrero de 2013, núm. 0/0, Nº Rec. 311/2011, (Marginal: 2416985)
- Sentencia de la Audiencia Nacional de fecha 19 de diciembre de 2012, núm. 0/0, Nº Rec. 530/2011, (Marginal: 2416983)

o Encargado que tenga un establecimiento en un país miembro de la UE y los Tratamientos por parte de una Responsable o Encargado **que, aunque no está establecido en la UE**, sus actividades están relacionadas con la oferta de bienes y servicios a interesados residentes en la UE

El GDPR incorpora una serie de novedades con el fin de dar un paso más en la protección de los datos personales. En general, lo que pretende la nueva normativa es evitar el mero cumplimiento por parte de los responsables mediante formularios tipo, o por la inscripción de los ficheros en la Agencia Española de Protección de Datos y quiere garantizar un análisis detrás de cada actuación, tratamiento y medida que se realice.

Las principales novedades que afectarán a los responsables son las siguientes:

NUEVOS PRINCIPIOS

Responsabilidad proactiva

Se refleja en la necesidad de que el responsable del Tratamiento demuestre que se cumple con lo dispuesto en el RGPD y que aplica medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD. En términos prácticos, **este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo**. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

En resumen, este principio exige una actitud consciente diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo. Todas las empresas deben estar en disposición, no sólo de cumplir, sino también de demostrar y documentar todos los requerimientos.

Privacidad desde el diseño y por defecto

Los responsables tendrán la obligación de **diseñar desde el inicio un proyecto, negocio, producto o servicio pensando en el cumplimiento y la protección de los datos personales y** adoptar medidas que garanticen que sólo se tratan datos necesarios (cantidad, extensión, periodos de conservación, accesibilidad de datos).

Es decir, tener en cuenta la privacidad a la hora de diseñar un tratamiento de datos y obrar siempre respetando la normativa, garantizando que se respeta la privacidad por defecto.

Transparencia

Debe informarse al interesado de las finalidades en un lenguaje claro, fácilmente comprensible.

La información que se ponga a disposición de los interesados deberá ser una información simple, comprensible y de fácil acceso.

Principio de minimización

Los datos personales solo se deben de tratar en caso de que no se pueda lograr la finalidad por otros medios.

NUEVAS OBLIGACIONES

Consentimiento

Uno de los cambios más importantes que nos trae el GDPR, y que, a su

vez, genera más preocupación a los responsables del tratamiento y en los profesionales del sector, es los requisitos para la obtención del consentimiento.

El GDPR prohíbe el consentimiento tácito o presunto (como las casillas premarcadas, el silencio o la inacción), y es obligatorio el **consentimiento inequívoco**, que es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa.

El Delegado de Protección de Datos (DPO)

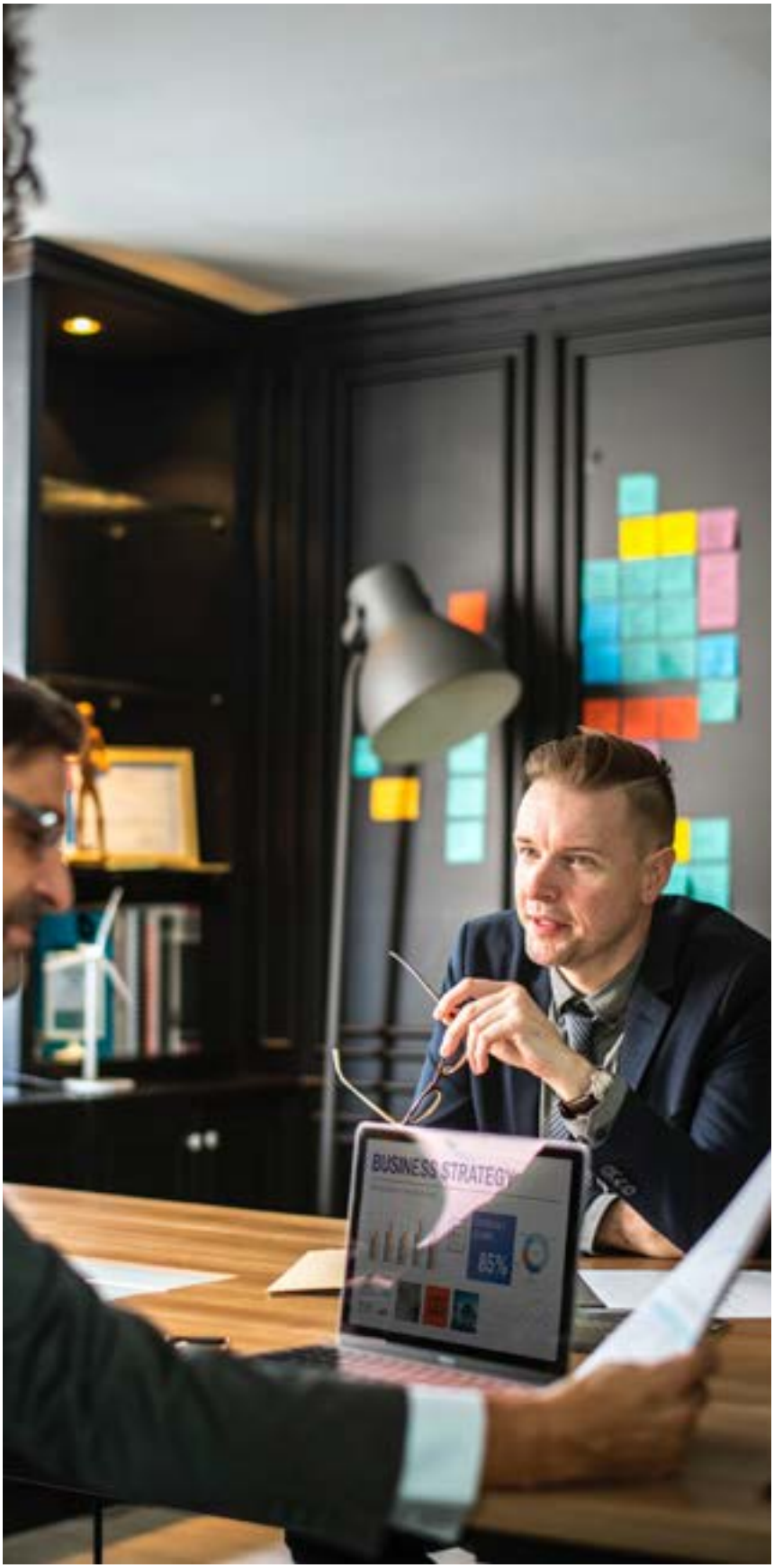
La designación del DPO no es obligatorio para todas las organizaciones, como, por ejemplo, para los despachos de abogados pequeños y medianos. Los casos en los que será necesario designar a un delegado son:

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

2. Cuando las actividades principales del responsable o del encargado del tratamiento de datos de carácter personal **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**.[1]

3. 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 y de **datos relativos a condenas e infracciones penales** a que se refiere el artículo 10 del Reglamento.

Además, el DPO tiene que reportar al máximo órgano jerárquico (Con-



1 El Reglamento no determina qué debe entenderse por "gran escala".

> **"Todas las empresas, despachos y profesionales autónomos se ven afectados por el nuevo Reglamento y deben implantar los nuevos principios y obligaciones en materia de privacidad"**

sejo de Administración o similar) lo cual recuerda mucho a la figura del ***"compliance officer"*** que asume unas funciones similares en la parte de prevención de riesgos penales y cumplimiento normativo. Es muy factible que en algunas organizaciones el ***"compliance officer"*** y el DPO recaigan en la misma persona o en el mismo órgano.

En el caso de pequeñas organizaciones, puede ser aconsejable que el DPO sea externo y se establezca una relación de "encargo de tratamiento" con plenas garantías entre el responsable y el DPO.

El DPO requiere una cualificación que incluya conocimientos jurídicos, técnicos, de gestión de programas y de gestión de riesgos, así como habilidades de comunicación. Podrá ser interno, externo o mixto. Esta última figura quizás puede ser la más adecuada contando para ello con un profesional en el que el DPO interno pueda apoyarse en su día a día.

Sus funciones son:

1. Informar y asesorar al responsable o al encargado de tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que existan en materia de protección de datos. Esta es quizás una de las funciones que en muchos casos venía adoptando el responsable de seguridad en muchas organizaciones.

2. Supervisar el cumplimiento de lo dispuesto en el Reglamento y de otras normativas de protección de datos incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento y las auditorías correspondientes.

3. Ofrecer asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

4. Cooperar con la autoridad de control.

Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa prevista en el Reglamento

Registro de actividades

Los responsables del tratamiento de datos de carácter personal en cada empresa deberán mantener un registro actualizado y por escrito de las actividades de tratamiento efectuadas bajo su responsabilidad, según lo dispuesto por el artículo 30, en los siguientes supuestos:

1. Cuando se trate de una **empresa con 250 empleados o más**

2. Cuando **el tratamiento no ocasional** que se realice pueda entrañar **un riesgo para los derechos y libertades de los interesados**

3. O cuando el **tratamiento** incluya **categorías especiales de datos personales**, relativos a **condenas** y/o a **infracciones penales**

Esta nueva obligación **sustituye la obligación de inscripción de los ficheros en el Registro General de Protección de Datos de la AEPD**, que recogía la Ley 15/1999, de 13 de diciembre, Orgánica de Protección de Datos española, en su artículo 25 y siguientes, y en su reglamento de desarrollo, Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (RLOPD).

El registro de las actividades de tratamiento deberá contener la siguiente información:

- La información del responsable (datos de identificación y de contacto)
- Los fines del tratamiento
- Una descripción de las categorías de interesados y de datos personales que se tratan
- Las categorías de destinatarios a quienes se comunican los datos personales (empresas del grupo, otros y/o transferencias internacionales)
- Los plazos previstos para la supresión de los datos recogidos/tratados
- Una descripción general de las medidas técnicas y organizativas de seguridad.

Análisis de riesgo y evaluacion de impacto

Todos los responsables deben realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. Dicho análisis de riesgo deberá hacerse durante TODO EL CLICLO DE VIDA DEL TRATAMIENTO, pero, sobre todo, antes. Es esencial este análisis, para **determinar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad al riesgo**, ya que la nueva legislación, no prevé una lista tasada de medidas de seguridad estructuradas en función del nivel de seguridad.

En cambio, hay otras medidas como la **evaluación de impacto** que se condicionan al riesgo alto contra los derechos y libertades del interesado y que sólo será obligatoria para los siguientes casos tasados:

- **Decisiones automatizadas**, que originen efectos jurídicos sobre la persona a quien corresponden los datos personales o le afecten significativamente,
- **Tratamientos a gran escala de categorías especiales** de datos o de datos personales relativos a **condenas** e infracciones **penales** o medidas de seguridad conexas,
- Observación sistemática a **gran escala** de una **zona de acceso público,**
- Operaciones que, a criterio de la autoridad de control competente, impliquen un **alto riesgo para los derechos de los interesados** y
- Cualquier tratamiento de datos que, por su naturaleza, alcance, contexto o fines, implique un **alto riesgo para los derechos y libertades de las personas** físicas, y en particular si utiliza **nuevas tecnologías.**

Brechas de seguridad:

Cuando se produzca una violación de la seguridad de los datos, el responsable deberá notificarla a la autoridad de protección de datos competente, sin dilación indebida (dentro de las 72 horas siguientes

“Cuando se produzca una violación de la seguridad de los datos, el responsable deberá notificarla a la autoridad de protección de datos competente, sin dilación indebida”

a tener constancia). Si hay dilación en la notificación se deberá justificar. **Se deberá notificar a la Agencia, cuando constituya un riesgo para los derechos y libertades de las personas físicas.** Sin dilación indebida, y de ser posible, a más tardar 72h después que se haya tenido constancia de ella.

En algunos casos, también deberá notificarse a los interesados cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades. Si el responsable ha cifrado los datos, cuando el responsable haya tomado medidas ulteriores que garanticen que el riesgo es improbable de que se materialice, o cuando suponga un esfuerzo desproporcionado, no será necesario notificar.

En cualquier caso, se deberán documentar las violaciones de seguridad. Asimismo, en los casos en que la violación de seguridad entrañe un alto riesgo para los interesados, la notificación debe dirigirse también a ellos.

BIBLIOGRAFÍA

BIBLIOTECA

- PIÑAR MAÑAS, JOSÉ LUIS. *Reglamento general de protección de datos*. Ed. Reus. 2016
- LÓPEZ CALVO, JOSÉ. *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*. Ed Bosch. 2018

Disponible en www.casosreales.es

ARTÍCULOS JURÍDICOS

- BACARIA MARTRUS, JORDI. *Las novedades del reglamento general europeo de protección de datos.* Economist&Jurist Nº 201. Junio 2016(www.economistjurist.es)
- ORTEGA GIMÉNEZ, ALFONSO Y DOMENECH, JUAN JOSÉ GONZALO. *Las transferencias internacionales de datos de carácter personal en el nuevo reglamento general de protección de datos.* Economist&Jurist Nº 217. Febrero 2018 (www.economistjurist.es)
- JOAQUÍN MUÑOZ. *Principios de protección de datos: Licitud, lealtad, transparencia, minimización, exactitud, integridad y confidencialidad.* Economist&Jurist Nº 217. Febrero 2018. (www.economistjurist.es)

Derecho al olvido y a la portabilidad de datos

Los famosos derechos ARCO (ACCESO, RECTIFICACIÓN, CANCELACION Y OPOSICIÓN) no sufren modificaciones relevantes y siguen siendo vigentes.

Principalmente GDPR nos trae dos nuevos derechos, el **derecho al olvido**, que es la posibilidad de revocar el consentimiento otorgado para el tratamiento de los datos personales, así como de solicitar la supresión y eliminación de los datos personales; y el **derecho a la portabilidad de los datos**, que se refleja en la posibilidad que tiene el interesado en recibir sus datos personales en un formato estructurado y de uso habitual y de lectura mecánica, así como transmitirlos de responsable a responsable del tratamiento.

RÉGIMEN SANCIONADOR

El nuevo régimen sancionador prevé **importantes sanciones de hasta 20 M de euros o de hasta el 4% de la facturación mundial anual de la compañía**. Lo que se persigue, es que las sanciones sean efectivas, proporcionadas y disuasorias, por lo que el importe de las sanciones se fijará según las circunstancias de cada caso.

Se valorará:

- El grado de responsabilidad del responsable del Tratamiento
- La naturaleza, gravedad y duración de la infracción
- La relación entre la finalidad y la categoría de los datos tratados
- El número de interesados/usuarios afectados
- Los perjuicios ocasionados y las medidas tomadas para mitigarlos
- La intencionalidad, negligencia o reiteración
- Tipo y plazo de notificación de la incidencia
- Si existe cooperación con la AEPD y cumplimiento de resoluciones
- La adhesión a mecanismos de certificación y/o a códigos de conducta
- Y los beneficios obtenidos o pérdidas evitadas.

Destacar, además, que el artículo 83 del GDPR, especifica que las multas serán *"efectivas,* ***proporcionadas*** *y disuasorias"*. La Agencia Española seguirá realizando acciones de mera advertencia y recordatorios de deberes legales, previos al procedimiento sancionador. ■

CONCLUSIONES

- El GDPR incorpora una serie de novedades con el fin de dar un paso más en la protección de los datos personales. En general, lo que pretende la nueva normativa es evitar el mero cumplimiento por parte de los responsables mediante formularios tipo, o por la inscripción de los ficheros en la Agencia Española de Protección de Datos y quiere garantizar un análisis detrás de cada actuación, tratamiento y medida que se realice