

## Sumario

### ANÁLISIS MONOGRÁFICO DEL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

#### **I PROTECCIÓN DE DATOS: El nuevo Reglamento de protección de datos entrará en vigor el 25 de mayo de 2018**

Autor: Luis Marimón

El 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 (RGPD) resultará **de plena aplicación el próximo 25 de mayo del 2018**. Con este escenario normativo aumenta la responsabilidad de las organizaciones para garantizar el cumplimiento de las obligaciones en materia de protección de datos.

La tan nombrada LOPD (ley 15/1999) y su reglamento de desarrollo (RD 1720/2007) quedan sin efecto en la misma fecha de mayo de 2018.

El nuevo Reglamento europeo tiene como finalidad armonizar las normas de protección de datos en la UE y es de aplicación directa en todos los estados miembros. En los próximos meses esperamos una nueva ley española de protección de datos que, a diferencia de la anterior, solo va a regular algunas

cuestiones menores, correspondiendo el grueso de la regulación al nuevo Reglamento europeo.

Este nuevo Reglamento **introduce novedades muy relevantes** en el sistema de protección de datos. Como muestra, desaparecen tanto la inscripción de ficheros ante la Agencia de Protección de datos (auténtica pieza angular en la anterior regulación) como los documentos de seguridad que seguirán siendo válidos únicamente hasta el día 25 de mayo.



Las principales novedades que plantea el nuevo Reglamento europeo de protección de datos personales son las siguientes:

### 1) Análisis de riesgos

Por primera vez es necesario proceder a realizar un análisis de riesgos del tratamiento de datos identificando, evaluando y categorizando los riesgos potenciales en función de su probabilidad y criticidad.

### 2) Principios básicos de la protección de datos

Los datos personales deberán ser:

- ☐ Tratados de manera lícita, leal y transparente en relación con el interesado.
- ☐ Recogidos con fines determinados, explícitos y legítimos.
- ☐ Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- ☐ Exactos y, si fuera necesario, actualizados.
- ☐ Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento.
- ☐ Tratados de tal manera que se garantice la seguridad adecuada de los datos personales.

### 3) Consentimiento

El consentimiento del afectado para el tratamiento de sus datos es uno de los ejes principales del mismo, aunque

tiene excepciones entre las que se encuentran las situaciones en las que el tratamiento es necesario para cumplir con lo previsto en un contrato o en una obligación legal (trabajadores o clientes, entre otros). El RGPD introduce una excepción en las situaciones en las que exista un **interés legítimo** de la empresa para mantener datos personales del afectado. Este principio aleja el consentimiento de algunas situaciones donde previamente era exigible.

El RGPD exige que el consentimiento sea expreso y que provenga de una actuación afirmativa por parte del usuario, lo que exige volver a analizar todos los consentimientos prestados antes de la entrada en vigor del Reglamento. El responsable del tratamiento tendrá la carga de la prueba para demostrar que el afectado prestó su consentimiento.



Otros principios relativos al consentimiento:

- ☐ El consentimiento se deberá prestar de forma independiente para cada finalidad.
- ☐ El consentimiento se podrá retirar en cualquier momento.

- El consentimiento tiene que proceder de una acción afirmativa, libre, informada e inequívoca. La acción afirmativa es nueva y parece descartar el consentimiento tácito válido hasta la fecha.

#### 4) Derechos de información

Se crean nuevos Derechos de información del afectado (anteriormente denominados derechos "ARCO"), además de los existentes hasta la fecha que se mantienen:

- **Derecho a la portabilidad de datos.** El interesado o un tercero designado por éste, podrá recibir los datos sujetos a tratamiento del interesado en un formato estructurado, de uso común y lectura mecánica.
- **Derecho a la limitación del tratamiento.** El interesado puede obtener del responsable del tratamiento la limitación de datos sujetos a tratamiento cuando impugne la exactitud de los mismos, o cuando el interesado se haya opuesto al tratamiento mientras se verifica si existen motivos legítimos que prevalezcan sobre los del interesado.

En el suministro de información, al recoger datos personales, hay que proporcionar más información que antes, por ejemplo, en relación con el plazo de conservación de datos o la posibilidad de presentar una reclamación ante la autoridad de control.

#### 5) Contratos de encargo del tratamiento

Se refuerza la necesidad de suscribir un contrato entre el responsable del tratamiento y el encargado del tratamiento, en los casos en los que el encargado del tratamiento tuviera acceso o tratara datos por cuenta del responsable, y con la finalidad de prestarle un servicio. Entre los nuevos puntos a considerar en el contrato del encargado del tratamiento:

- La exigencia al responsable del tratamiento de contratar los servicios solamente a encargados del tratamiento que proporcionen garantías suficientes de que la información y los datos van a ser tratados de forma adecuada.
- El sub encargo del tratamiento por parte del encargado, requiere autorización del responsable salvo pacto previo por escrito.
- El encargado pondrá a disposición del responsable toda la documentación necesaria que acredite que el encargado ha cumplido con lo previsto en el RGPD, así como para permitir auditorías de control.
- El sub encargo del tratamiento requiere la firma de un contrato entre el encargado y el sub encargado. El encargado continuará siendo responsable de todas sus funciones y también de las que asuma el sub encargado.

## 6) Registro de actividades del tratamiento

Todas las empresas de más de 250 empleados tienen la obligación de mantener un registro de actividades del tratamiento. En este registro de actividades del tratamiento se debe incluir, entre otros, la siguiente información:

- Datos de contacto.
- Listado de procesos internos que incluyan datos personales.
- Encargados del tratamiento.
- Transferencias internacionales.
- Plazos de supresión.
- Medidas de seguridad.

Este registro de actividades del tratamiento debe estar permanentemente actualizado y disponible para la autoridad de control en caso de que lo requiriera.

## 7) Delegado de Protección de Datos (DPO)

Las empresas deberán nombrar un Delegado de Protección de datos (*Data privacy officer*: DPO, en inglés) en el caso de que almacenen o traten un volumen elevado de datos o se dediquen a determinadas actividades previstas en la norma. En todo caso, se aconseja el nombramiento de un DPO en aquellas empresas que almacenen y traten datos en grandes volúmenes, o datos de gran sensibilidad.

Si se nombrara un DPO, éste tendrá las siguientes funciones:

- ☞ Informar y asesorar en materia de protección de datos en la empresa.

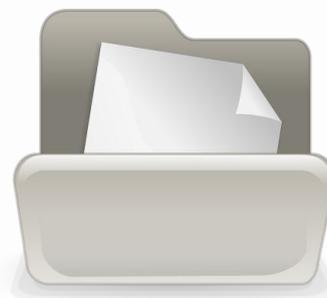
- ☞ Supervisar el cumplimiento de políticas internas incluyendo la formación del personal de la empresa.
- ☞ Cooperar y actuar como punto de contacto con la autoridad de protección de datos.

El DPO debe ser una persona experta en Derecho y con formación específica en materia de protección de datos.

## 8) Principio de *accountability*

Se introduce el principio de *accountability* por el que el responsable del tratamiento queda obligado a implementar medidas técnicas y organizativas tendentes a **demostrar el cumplimiento** de lo dispuesto en el RGPD, por parte de la empresa y a revisar y actualizar las medidas cuando resulte necesario.

En nuestra opinión, este principio acerca los proyectos de protección de datos a proyectos de *compliance* en los que las actividades internas en materia de datos personales incluyendo la creación, modificación y destrucción de procesos junto con todas las revisiones, deben quedar debidamente registradas y documentadas.



## 9) Protección de datos desde el diseño y por defecto

El nuevo RGPD introduce dos conceptos nuevos:

**Protección de datos desde el diseño:** El Reglamento pretende que la política de protección de datos de cada empresa se tenga en cuenta de forma incipiente, en el momento de diseñar los productos, servicios o procedimientos internos o externos, como parte del diseño de los mismos, teniendo en cuenta el estado de la técnica, el coste de la operación y la naturaleza, ámbito, contexto y fines del tratamiento.

**Protección de datos por defecto:** cuya finalidad es garantizar que solo sean objeto de tratamiento los datos que realmente sean necesarios a fin de garantizar la necesidad de la empresa y los fines específicos de tratamiento. Esta obligación se aplica a la cantidad de datos personales recogidos como a la extensión de su tratamiento, el plazo de conservación y su accesibilidad.

## 10) Notificaciones de brechas de seguridad

La norma exige que en el plazo máximo de 72 horas se notifique a la autoridad de control cualquier brecha de seguridad que pueda afectar a la empresa. Se considera brecha de seguridad cualquier situación en la que exista una violación de la seguridad de los datos personales que entrañe un alto riesgo para los derechos y libertades de las personas físicas.

## 11) Evaluaciones de impacto

El RGPD establece también como novedad la necesidad de realizar evaluaciones de impacto (*Privacy Impact*

*assessment*: PIA, en inglés) en determinados casos. El objetivo de las PIA es realizar un análisis en profundidad en los casos en los que se vislumbran potenciales operaciones de procesamiento de datos que impliquen alto riesgo. El propio RGPD establece que podría existir alto riesgo en: “la evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de forma similar”. Es importante realizar una PIA en casos de uso de nuevas tecnologías a gran escala o en caso de tratamiento relevante de datos sensibles. La PIA deberá contener una descripción de las operaciones de datos previstas y las finalidades del tratamiento, un análisis de la necesidad y proporcionalidad de las operaciones de tratamiento, la evaluación de riesgos para los derechos y libertades de los interesados y las medidas previstas para afrontar los riesgos.

## 12) Conclusión

De la lectura de los puntos anteriores y de otras medidas previstas en el nuevo Reglamento se deduce claramente que la protección de datos debe ocupar un papel cada vez más relevante en las empresas y que tiene que formar parte de la cultura empresarial como ya ocurre, por ejemplo, con la prevención de riesgos laborales.

---

Desde [este enlace](#) pueden acceder a la Guía para la Adaptación al Reglamento europeo de protección de datos (RGPD), que preparamos hace unos meses. Nuestro despacho desarrolla procesos de adaptación al nuevo Reglamento y estaremos encantados de atender las consultas sobre la introducción del mismo.

# Marimón Abogados

Marimón Abogados es un despacho fundado en 1931 que ofrece servicios legales en todas las áreas del Derecho y que cuenta con oficinas en Barcelona, Madrid y Sevilla. Nuestro despacho se ha adaptado a los cambios que se han ido produciendo en el mercado mediante la mejora constante de sus servicios y la ampliación de sus ramas de actividad, creando departamentos altamente especializados que cuentan con una vasta experiencia, lo que nos permite resolver cualquier tema legal desde la misma firma:

<a href="#">Administrativo, Regulatorio, Urbanismo y Medio ambiente</a>	<a href="#">Concursal</a>	<a href="#">Financiero</a>	<a href="#">Fiscal</a>
<a href="#">Inmobiliario</a>	<a href="#">Laboral</a>	<a href="#">Mercantil y Societario</a>	<a href="#">Penal</a>
<a href="#">Procesal</a>	<a href="#">Propiedad Intelectual e Industrial</a>	<a href="#">Tecnologías de la Información y Protección de Datos</a>	<a href="#">Competencia</a>
<a href="#">Italian Desk</a>	<a href="#">French Desk</a>	<a href="#">German Desk</a>	<a href="#">Portuguese Desk</a>

Para cualquier aclaración o comentario sobre el contenido de esta información pueden ponerse en contacto con los siguientes abogados:



**Luis Marimón**

Departamento de Derecho mercantil y responsable del área de IT/IP.

[imarimon@marimon-abogados.com](mailto:imarimon@marimon-abogados.com)



**Eduard Blasi**

Departamento especializado en IT/IP y experto en protección de datos.

[blasi@marimon-abogados.com](mailto:blasi@marimon-abogados.com)



## Barcelona

Paseo de Gracia 118, 5º  
08008 Barcelona  
Tel.: (+34) 93 415 75 75



## Madrid

Paseo de Recoletos, 16, 4º  
28001 Madrid  
Tel.: (+34) 91 310 04 56



## Sevilla

C/ Balbino Marrón 3, 5º, of. 17  
41018 Sevilla  
Tel.: (+34) 95 465 78 96

*Este documento es una recopilación de información jurídica elaborada por Marimón Abogados. La información que se incluye en el mismo no constituye asesoramiento jurídico. Los derechos de propiedad intelectual sobre este documento son propiedad de Marimón Abogados. Queda prohibida la reproducción en cualquier medio, la distribución, la cesión y cualquier otro tipo de utilización de este documento, ya sea en su totalidad, ya sea de forma extracta, sin la previa autorización de Marimón Abogados.*