

**Guía de obligaciones** para las empresas  
en el cumplimiento del Reglamento (UE)  
2016/679 de Protección de Datos de  
Carácter Personal

## La normativa

El artículo 18.4 de la Constitución dice que *“la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*.

Con la intención de hacer realidad este artículo nace la Ley Orgánica 5/1992, conocida como LORTAD, posteriormente derogada por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, y actualmente todo ello se verá modificado/derogado por el **Reglamento (UE) 2016/679** del consejo de 27 de abril de 2016, y el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (121/000013).

### En caso de incumplimiento

- ✓ **Multas económicas de hasta 20 millones de euros** o la cuantía equivalente al **4% del volumen de negocio total anual**.
- ✓ **Indemnizaciones por daños y perjuicios** (art. 82 del RGPD).
- ✓ **Responsabilidades penales** por parte del responsable en función del tipo de infracción.

No se puede poner en tela de juicio las enormes ventajas que nos reporta el uso de la informática en nuestra actividad empresarial, mejorando y aumentando tanto la productividad personal como la de las empresas. Sin embargo, quién no se ha preguntado alguna vez si aquellas empresas que tratan sus datos, con ordenadores cada vez más potentes y con bases de datos con mayor volumen de información, no tendrán demasiada información sobre su vida privada y qué uso harán de la misma.

Como ciudadanos nos preocupa relativamente el tratamiento de los datos de carácter personal cuando son de carácter básico (nombre, dirección, teléfono...), pero ¿y cuando se trata de datos más sensibles? (renta, solvencia, recibos, afiliación sindical o política, salud, vida sexual...).

Toda esta información nos ofrece perfiles y hábitos precisos sobre las personas, perfiles que en algunos casos ni el propio titular de los datos conoce y que pueden ser utilizados de manera inadecuada. Solo debemos valorar la información que se puede obtener de una persona conociendo sus movimientos bancarios, obteniendo información precisa sobre sus actividades de ocio y gustos, vida familiar, capacidad económica y un largo etcétera; o si analizamos la factura telefónica cruzando los datos que posee el operador de telefonía con las llamadas que realiza.

La intimidad es un valor que se reconoce de forma unánime en todo el mundo civilizado desde el siglo XX, los límites sobre la tenencia y utilización de los datos de carácter personal, así como el tráfico de los mismos quedan reflejados en la Legislación sobre Protección de datos, afectando a todas las organizaciones que constituyen el tejido empresarial de nuestro país, ya que todas manejan datos de este tipo (clientes, proveedores, empleados, asesores externos...).

Es por ello que **todas las empresas deben adaptarse a la legislación** teniendo en cuenta que deben conjugar, por un lado, los derechos que poseen los ciudadanos sobre el uso, tratamiento y destino de sus datos y, por otro lado, las medidas de tipo organizativo-técnico que debemos conferir a dichos datos en nuestra organización.

El planteamiento de este dossier es facilitar a nuestro colectivo la correcta comprensión de la Ley, así como las obligaciones que se establecen y deben adoptar.

## Legislación aplicable

**Reglamento (UE) 2016/679** del consejo de 27 de abril de 2016 a través de sus 49 artículos la presente ley tiene por objeto *“establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos, así como proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales”*.

**El Proyecto de Ley Orgánica de Protección de datos** de carácter personal (121/000013). Tiene por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

**Las Recomendaciones dictadas por el Director de la Agencia** con objeto de adecuar el funcionamiento de ciertos sectores de actividad a la normativa española de protección de datos. Son elaboradas tras la realización de los Planes Sectoriales de Inspección de Oficio que anualmente desarrollan.

**Las instrucciones dictadas por la Agencia Española de Protección de Datos**, cuya finalidad es aclarar y apoyar la interpretación de la ley con el fin de adecuar los tratamientos a sus principios.

## ¿A quién afecta esta normativa?

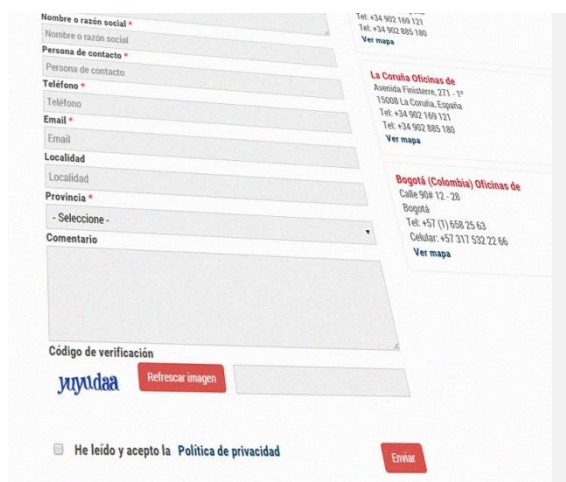
Aplicable a todos los profesionales liberales, empresas y organizaciones públicas o privadas que almacenen, utilicen o traten datos de carácter personal registrados en soporte físico y que los haga susceptibles de tratamiento.

Considerándose “datos de carácter personal” a cualquier información concerniente a personas físicas identificadas o identificables. **Todas las empresas manejan este tipo de datos** en el desarrollo de su actividad; debemos tener en cuenta que una relación de clientes o proveedores de una base de datos o la relación de trabajadores de su empresa, son ficheros de carácter personal, afectados por las normativas anteriormente citadas.

Uno de los principios básicos en los que deben apoyar su comprensión de la legislación en materia de protección de datos, es que los datos que tratan en su empresa no son propiedad de la misma, sino de sus titulares, por lo que para la correcta aplicación de la normativa debemos tener en cuenta las **tres fases en las que se estructura el tratamiento de los datos en la empresa:**

- a) El momento de la recogida de datos.
- b) Durante el tratamiento de los mismos.
- c) El momento de la utilización y cesión o comunicación a terceros.

Las obligaciones de las empresas no se reducen a un momento puntual, **es un proceso constante en el tiempo** que afecta a su actividad empresarial.



The image shows a contact form with the following fields: 'Nombre o razón social', 'Persona de contacto', 'Teléfono', 'Email', 'Localidad', 'Provincia', and 'Comentario'. Below these is a 'Código de verificación' field with a 'Refrescar imagen' button. At the bottom, there is a checkbox for 'He leído y acepto la Política de privacidad' and an 'Enviar' button. To the right of the form, there are two location cards. The first is for 'La Coruña Oficinas de' at 'Avenida Feixas, 271 - 1º, 15008 La Coruña, España', with phone numbers '+34 982 169 121' and '+34 982 085 180'. The second is for 'Bogotá (Colombia) Oficinas de' at 'Calle 50# 72 - 28, Bogotá', with phone numbers '+57 (1) 658 25 63' and '+57 311 532 22 66'.

## La Agencia Española de Protección de Datos (AEPD)

Su **misión es la de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación**, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. Es un ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta normativa nacional en materia de protección de datos y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea

Cualquier actuación contraria a las obligaciones contenidas en la RGPD puede ser objeto de denuncia ante la AEPD, estableciéndose las posibles infracciones en leves, graves y muy graves, con un abanico de **sanciones** que pueden ser de **hasta 10 millones de euros o el 2% del VNA** en los casos más leves o de **hasta 20 millones de euros o el 4% del VNA** en los casos más graves.

Es importante tener en cuenta que la cuantía de las sanciones económicas va a parar a la Administración y no al afectado, aunque este luego tendrá derecho a recibir una **indemnización por los daños y perjuicios** sufridos del Responsable o encargado del tratamiento que comete el acto infractor.

Las correspondientes acciones judiciales en el ejercicio del derecho a indemnización se presentarán ante los tribunales competentes, no ante la Autoridad de Control.

Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

- a) El carácter continuado de la infracción.
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
- c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
- d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
- e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

## Obligaciones de las empresas

Las obligaciones más reseñables a cumplir por parte de la empresa deben dividirse en obligaciones como **responsable del tratamiento** y como **encargado de tratamiento**, es decir, existirán obligaciones propias (registro de actividades, cumplimiento de principios básicos, evaluación del impacto, medidas de seguridad, comunicaciones de violaciones de seguridad, definición del Delegado de Protección de Datos cuando proceda, entre otros) y aquellas que se deriven de un contrato de tratamiento (registro de actividades, medidas de seguridad y designación del DPO principalmente).

A grandes rasgos, existen tres obligaciones principales a cumplir por parte de la empresa (responsable del tratamiento) en el cumplimiento del RGPD y cuya finalidad es impedir el mal uso o abuso de la información que trate.

### **Obligaciones principales de las empresas:**

1. *Responsabilidad proactiva*
2. *Atención a los derechos del ciudadano*
3. *Funciones y obligaciones del personal*

## 1. Responsabilidad proactiva

Se traduce en la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme al Reglamento.



### 1.1 Análisis de la necesidad EIPD

Se trata de un procedimiento que busca la valoración de la conveniencia de llevar a cabo, o no, una Evaluación de Impacto en la Protección de Datos Personales.



### 1.2 Análisis de riesgo

El Responsable del Tratamiento deberá realizar un Análisis de Riesgos de los tratamientos que realice, para definir las **medidas a aplicar y cómo implementarlas**. Se analizarán en base a determinados criterios como: tipo de datos, número de interesados afectados, cantidad y variedad de tratamientos, uso de tecnologías invasivas, etc.

El objeto del análisis de riesgos es **determinar las medidas u obligaciones concretas** que la entidad debe implementar, entre otras, la designación del Delegado de Protección de Datos, la evaluación de impacto, las medidas concretas de seguridad, las medidas en caso de realizar transferencias internacionales de datos, etc.



### 1.3 Evaluación del Impacto sobre la Protección de Datos (EIPD)

Es un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de los datos personales evaluándolos y determinando las medidas para abordarlos

**Respecto a qué:** Para tratamientos que entrañen un ALTO riesgo para los derechos y libertades de los interesados.

**Cuándo:** Con carácter previo al inicio del tratamiento

**Para qué:** determinar las medidas técnicas y organizativas necesarias y adecuadas para velar por la seguridad de la información

En todo caso, la evaluación deberá realizarse en tres supuestos que se consideran de Riesgo Alto:

1. **Elaboración de perfiles** sobre cuya base se tomen decisiones que produzcan efectos para las personas jurídicas.
2. **Tratamiento a gran escala** de datos sensibles.
3. **Observación sistemática a gran escala** de una zona de acceso público.

Las autoridades de control también podrán establecer listas de operaciones de tratamientos sometidas a EIPD.



#### 1.4 Registro de actividades

El Responsable del Tratamiento y el Encargado del Tratamiento deberán llevar un **registro de las actividades de tratamiento** que se encuentren bajo su responsabilidad. Están **obligados a llevar a cabo este registro**

1. Organizaciones o empresas que empleen a **más de 250 trabajadores**.
2. Organizaciones o empresas que realicen **tratamientos de datos** con las siguientes características:
  - a. **Tratamientos que puedan ocasionar un riesgo** para los derechos y libertades de los interesados.
  - b. **Tratamientos de categorías especiales** de datos o aquellos relativos a **condenas e infracciones penales**.
  - c. **Tratamientos que no sean ocasionales**.



#### 1.5 Protección de datos desde el diseño y por defecto

Por un lado cuando hablamos de **protección de datos desde el diseño** nos referimos a la aplicación y definición de medidas en materia de protección de datos desde el momento en que se diseña o se determinan los medios del tratamiento, así como, mientras se realiza el propio tratamiento.

Teniendo en cuenta lo siguiente:

- El estado de la técnica.
- El coste de aplicación.
- La naturaleza del tratamiento.
- El ámbito de aplicación.
- El contexto.
- Las finalidades del tratamiento.
- Los riesgos para los derechos y libertades.

Por otro lado cuando hablamos de **protección de datos por defecto** nos referimos a la aplicación y definición de medidas técnicas y organizativas apropiadas y necesarias para los fines concretos del tratamiento (principio de minimización).

Teniendo en cuenta:

- La cantidad de datos recogidos.
- La extensión de su tratamiento.
- El plazo de conservación.
- La accesibilidad.





## 1.6 Medidas de Seguridad

Los responsables o encargados del tratamiento establecerán las medidas técnicas y organizativas apropiadas para **garantizar un nivel de seguridad adecuado** en función de los riesgos detectados en el análisis previo.

Las medidas de seguridad deberán garantizar, al menos:

- ✓ **Seudonimización y cifrado de datos.**
- ✓ Capacidad para garantizar la **confidencialidad, integridad, disponibilidad y resiliencia** permanente.
- ✓ Capacidad de **restaurar la disponibilidad** y el **acceso a los datos**.
- ✓ Proceso de **verificación, evaluación y valoración** regulares de la eficacia de las medidas.



## 1.7 Notificación de violaciones de seguridad

Todo incidente que ocasione la **destrucción, pérdida o alteración accidental o ilícita de datos personales** transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Ante cualquier violación de seguridad, el responsable deberá:

- ✓ Documentar las violaciones de seguridad.
- ✓ Violaciones que entrañen un alto riesgo.
- ✓ Notificación a la Autoridad de Control competente.
- ✓ Comunicación a los interesados.



## 1.8 Delegado de protección de datos (DPO)

El Delegado de Protección de Datos es una nueva figura que incorpora el Reglamento que deberá estar perfectamente integrada en el organigrama de la entidad con la intención de conocer y coordinar todo lo que tenga que ver con la protección de datos de la entidad, determinando y organizando las políticas de protección, los protocolos en los tratamientos de datos y asegurar que todo se desarrolle conforme a la normativa.

Se trata de una **figura obligatoria** en los siguientes casos:

- ✓ Para **autoridades y organismos públicos**.
- ✓ Para responsables o encargados de tratamiento con actividades que requieran un **seguimiento regular y sistemático de interesados a gran escala**.
- ✓ Para responsables o encargados de tratamiento que lleven a cabo **tratamientos a gran escala de categorías especiales de datos o datos personales relacionados con condenas y delitos penales**.



«Se designará en función de su cualificación profesional y, en especial, su conocimiento experto de la legislación y las prácticas de protección de datos así como su capacidad de desempeñar las tareas a las que hace referencia el artículo 39».

## 2. Atención a los derechos del ciudadano

El tratamiento de los datos de carácter personal puede suponer una acumulación de información que posibilite definir un perfil de la persona fuera de su control. Para minimizar este riesgo, se conceden a los ciudadanos **derechos** que le otorguen la facultad de poder ejercer un control sobre el uso de sus datos. Estos derechos son: **acceso, rectificación, supresión (derecho al olvido), oposición, portabilidad de los datos y derecho a la limitación** de los considerándose todos ellos principios fundamentales sobre los que se asienta la ley.

Cada uno de los derechos es independiente de los demás, pudiendo ejercerse libre y gratuitamente; el ejercicio de cualquiera de ellos no es requisito previo para el ejercicio de otro.

Para ejercitar estos derechos es necesario, por parte del titular de los datos, el cumplimiento de unos requisitos formales básicos, como es la entrega o envío de una solicitud al responsable del tratamiento que contenga los nombre y apellidos, fotocopia del DNI y la petición en la que se concreta la solicitud.

El Responsable del Tratamiento debe estructurar **procedimientos lógico-administrativos** que permitan el ejercicio de los legítimos derechos de los ciudadanos, preocupándose de establecer los cauces o vías de respuesta a dichas solicitudes, así como el debido conocimiento por parte del personal de la empresa a través de formación o concienciación de las obligaciones a las que están sometidos.

Con el objetivo de dar amparo a los derechos de las personas físicas en cuanto a la protección de sus datos personales se refiere, la normativa vigente en materia de protección de datos, concretamente el Reglamento General de Protección de datos (RGPD) ha establecido una serie de infracciones que llevarán aparejadas sus correspondientes sanciones.

En este sentido, el artículo 83.5 del RGPD, tipifica como infracción grave el incumplimiento de todo lo dispuesto en relación a la atención a los derechos de los interesados.

En este sentido, este tipo de infracciones son sancionables con multas administrativas de 20.000.000 de euros como máximo o, tratándose de una empresa, de cuantía



equivalente al 4% como máximo del volumen de negocio anual global del ejercicio financiero anterior, optando por la de mayor cuantía.

### 3. Funciones y obligaciones del personal

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas de acuerdo con lo establecido en el RGPD.

El Responsable del fichero adoptará las **medidas necesarias para que el personal conozca las normas de seguridad** que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.

Es clave dentro de la correcta adaptación a la RGPD, la concienciación y formación de los usuarios que tengan acceso a datos de carácter personal, haciéndolos conocedores de la importancia y seriedad de la normativa y formándolos sobre las funciones, obligaciones y normas que deben cumplir; sin la consecución de estos puntos la adaptación no será exitosa.

La adaptación puntual de la compañía a la RGPD y la Seguridad informática no es una vacuna que protegerá indefinidamente sus sistemas, por lo que se deben auditar y corregir de manera permanente las medidas, procedimientos y sistemas de información establecidos.

La falta de un proceso de concienciación y formación adecuados provocan, con mucha frecuencia, que nuestro propio personal de forma voluntaria o involuntaria sea la principal fuente de errores en materia de protección de datos y seguridad, de tal modo que una parte muy importante de las sanciones de la Agencia están provocadas por una mala praxis del personal de la organización.

## Conclusiones

La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

El uso generalizado de la informática ha hecho que los Estados legislen para salvaguardar la intimidad de sus ciudadanos. España ha reaccionado imponiendo estrictos requisitos y fuertes sanciones, de las más elevadas de la Unión Europea; como consecuencia, las empresas deben optar por gestionar prudentemente los datos personales que obran en su poder.

La aplicación de la RGPD en las organizaciones viene dada por un motivo fundamental que consiste en evitar las elevadísimas sanciones previstas en la RGPD que pueden ser de hasta 10 mil o el 2% del VNA en los casos más leves o de hasta 20 mil o el 4% del VNA en los casos más graves.

pero no debemos olvidar que al cumplir la ley, no solo mejoramos la seguridad y procedimientos de nuestra organización, sino también la imagen frente a nuestros clientes, proveedores y empleados, respetando la privacidad y el derecho a su intimidad.

Conviene tener presente que los servicios de consultoría externos asisten, ayudan y complementan al empresario a una personalizada y rápida adaptación a la legislación en materia de Protección de Datos, pero nunca pueden sustituirle en la responsabilidad del cumplimiento de la normativa implementada en su organización.

---

### ¿Necesita ayuda para adaptarse al Reglamento de Protección de Datos?



Desde AYSE LUCUS SLP podemos brindarle nuestra experiencia durante 10 años ayudando a empresas como la suya a adaptarse a distintas normativas de protección de datos facilitándole la **asesoría** que necesite y **mantenimiento** su adaptación y **registro de su actividad** totalmente actualizados ante la Autoridad de Control competente.

Puede ponerse en contacto con nosotros a través de:

info@ayselucus.es | 982 87 13 55 | www.ayselucus.es

