

# LEY DE PROTECCIÓN DE DATOS



**En España existe desde el año 1999 una Ley Orgánica de Protección de Datos (conocida como LOPD) de obligado cumplimiento para aquellas empresas, entidades y Administraciones Públicas que manejen datos de carácter personal.**

**Desarrollada actualmente por el Real Decreto 1720/2007 de desarrollo de medidas técnicas y organizativas para garantizar la seguridad de los ficheros con datos personales automatizados o no.**



# ¿QUÉ NORMATIVA UTILIZAR COMO MARCO LEGAL?

- Las webs que realicen actividades mercantiles sin recogida de datos personales, deben ajustarse a la **Ley de Servicios de la Sociedad de la Información (en adelante, LSSI)**.
- Las webs que realicen recogida de datos personales pero no almacenamiento también tienen como marco la **LSSI**.
- Finalmente, las webs que, además de la recogida, realicen almacenamiento de datos personales deben ajustarse a la **LOPD**.



# ¿PROTECCIÓN DE DATOS?

**Derecho fundamental** de las personas consistente en un **poder de disposición y de control** sobre cualquier información concerniente a ellas mismas (su nombre, apellidos, dirección, número de teléfono, edad, datos bancarios, historial médico, ideología, etc.)



Solo la persona tiene el **derecho a decidir a quién y para qué** proporciona sus datos de carácter personal y no aquel que le solicita sus datos, no estando obligado a facilitarlos si no se desea, salvo que exista una ley que expresamente así lo disponga.

La **imagen** también es un dato de carácter personal, teniendo el derecho a decidir sobre su recogida, grabación y utilización.



Habría que tener en cuenta las obligaciones de las empresas respecto a los mencionados datos, siguiendo cronológicamente la vida de los mismos, es decir, desde el primer momento, el de **su recogida**, pasando por su **almacenamiento** (informático o no), **su tratamiento** y, finalmente, las **posibles comunicaciones a terceros del dato**, fuera del ámbito de actuación de la empresa.



# DATOS ESPECIALMENTE PROTEGIDOS

Hay datos que merecen una **protección reforzada** ya que forman parte de la esfera más íntima de las personas (por ejemplo datos relativos a la salud, historial médico, ideología, religión, creencias, origen racial o vida sexual). Para la recogida de estos datos se ha de contar con el **consentimiento expreso** de los titulares.



# CONCEPTOS FUNDAMENTALES

- **Datos de carácter personal:**

*“Cualquier información concerniente a personas físicas identificadas o identificables”*. (Art. 3.a LOPD).

- **Fichero:**

*“Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso”*. (Art. 3.b LOPD).

- **Tratamiento de datos:**

*“Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”*. (Art. 3.c LOPD).



- **Afectado o interesado:**  
“Persona física titular de los datos que sean objeto del tratamiento a que se refiere la definición anterior”. (Art. 3.e LOPD).
- **Consentimiento:**  
“Toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”. (Art. 3.h LOPD).
- **Cesión de datos:**  
“Toda revelación de datos realizada a una persona distinta del interesado”. (Art. 3.i LOPD).  
Ejemplos de cesiones de datos:  
*Se produce una cesión cuando los datos que se han obtenido para una determinada finalidad se ceden a un tercero para el ejercicio de otra finalidad distinta de aquella para la que se recogieron.*
- **Responsable del fichero:**  
“Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decide sobre la finalidad, contenido y uso del tratamiento”. (Art. 3.d LOPD).



- **Encargado de tratamiento:**

*“Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento”. Art. 3.g LOPD.*

*Un ejemplo típico de encargado del tratamiento es la empresa con la que podemos establecer una relación contractual para que se encargue de la destrucción de los documentos que contienen datos de carácter personal y ya no tengo por qué mantener en mis archivos.*

- **Procedimiento de Disociación:**

*“Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable”. (Art. 3.f LOPD).*

*Un ejemplo típico de disociación es el realizado para el desarrollo de funciones de estadística.*



- **Fuentes accesibles al público:**

*“Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación”. Art. 3.j LOPD.*

- **Usuarios:**

*Son usuarios el personal al servicio del responsable del fichero o encargado del tratamiento que tengan acceso a los datos de carácter personal como consecuencia de tener encomendadas tareas de utilización material de los datos almacenados o que se almacenarán en los ficheros.*

*Los usuarios están obligados al cumplimiento de las medidas de seguridad establecidas para el tratamiento de los datos y están sujetos al deber de secreto.*



# OBLIGACIÓN DE NOTIFICACIÓN DE FICHEROS

Cualquier entidad que disponga de ficheros donde se archiven datos de carácter personal tiene la obligación de notificación de los mismos ante la AEPD, así como notificar cualquier modificación o cancelación de dichos ficheros.



# LOS PRINCIPIOS DE LA PROTECCION DE DATOS:

## Principio de información

El personal de la empresa deberá abstenerse de recabar datos personales sin informar al interesado de los extremos recogidos en el art. 5 LOPD (existencia de un fichero, responsable del tratamiento, dirección, finalidad, lugar donde ejercitar sus derechos...)

Si el personal detectara ficheros con datos personales de interesados que no hayan sido debidamente informados, deberá ponerlo en conocimiento de la dirección con el objeto de subsanar la incidencia con la mayor celeridad.

La creación de ficheros con datos personales deberá estar expresamente autorizada por la dirección de la empresa.



# LOS PRINCIPIOS DE LA PROTECCION DE DATOS:

## Principio de consentimiento

El tratamiento de datos personales requiere el **consentimiento inequívoco previo** de los interesados.

Este consentimiento deberá ser expreso (firma) cuando se trate de datos especialmente protegidos (informes médicos previos al alta del trabajador en la empresa o los registros obligatorios según la normativa de PRL,...)

El personal de la empresa deberá recabar el consentimiento informado expreso y previo del interesado para el tratamiento de sus datos personales



# ¿QUIEN DEBE DAR ESTE CONSENTIMIENTO?

- a) **Si el usuario está plenamente capacitado para expresar libremente su consentimiento:** será el propio usuario quien actúe en nombre propio en todos los actos de disposición de sus datos.
- b) **Si el usuario está declarado incapaz por sentencia judicial firme:** será el representante legal o tutor, quien actúe en nombre del usuario.



# LOS PRINCIPIOS DE LA PROTECCION DE DATOS:

## Principio de calidad de los datos

Los datos de carácter personal sólo se podrán recoger para su tratamiento, cuando sean **adecuados, pertinentes y no excesivos** en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Además, estos datos **no podrán utilizarse para finalidades incompatibles** con aquellas para las que hubieran sido recogidos, deben ser exactos y cancelados cuando dejen de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.



Los datos recogidos deben ser los imprescindibles para poder prestar el servicio del que se trate.

Pedir más datos de los estrictamente necesarios puede incitar desconfianza en el usuario que suministra sus datos.



# LOS PRINCIPIOS DE LA PROTECCION DE DATOS:

## Deber de secreto

El personal tiene el deber de guardar **secreto profesional y confidencialidad** de la información tratada.

Quién intervenga en cualquier fase del tratamiento de los datos de carácter personal está obligado al secreto profesional y al deber de guardarlos.

Estas obligaciones subsistirán aún después de finalizar sus relaciones con la empresa.



El personal deberá firmar un “**Compromiso de confidencialidad**”, donde se le informará de los deberes de confidencialidad de datos personales, tanto en la custodia como en el tratamiento de los datos personales responsabilidad de la empresa.

El personal sólo podrá acceder a ficheros con datos personales **relacionados con sus propias funciones**. Si el personal no requiere para sus funciones el acceso a datos personales, no podrá acceder a éstos.



La **vulneración del deber de guardar secreto** sobre los datos de carácter personal incorporados a ficheros que contengan datos personales será considerada como una **falta leve, grave o muy grave** de conformidad con lo previsto en la LOPD, lo cual daría lugar a iniciación de actuaciones disciplinarias, si procediesen.



# LOS PRINCIPIOS DE LA PROTECCION DE DATOS:

## Cesiones de datos

La regla general establecida por la LOPD, para la cesión o comunicación de datos a terceros responde a una doble necesidad:

- a) Que exista el **consentimiento previo de la persona afectada.**
  
- b) Que la cesión de los datos responda al cumplimiento de **fines directamente relacionados con las funciones legítimas del cedente y del cesionario.**



# CESIONES DATOS AMPARADAS EN LEY

a) **Cuando una Ley lo prevea**, por ejemplo, en el caso de tener que comunicar a un juez una serie de datos personales porque dicho sujeto se encuentra inmerso en un procedimiento judicial.



b) También se podrán ceder datos, además de a los Juzgados, a los siguientes organismos siempre que una Ley así lo prevea: administraciones públicas competentes; Hacienda Pública, Defensor del Pueblo o al Tribunal de Cuentas o a los órganos equivalentes en cada Comunidad Autónoma.



c) Cuando la cesión de datos responda a la **libre y legítima aceptación de una relación jurídica que implica la conexión del tratamiento con ficheros de terceros**. A efectos de ejemplo, se incluiría:

- **Despachos profesionales o gestorías, bancos** siempre que la empresa contrate sus servicios profesionales para el cumplimiento de las legítimas finalidades de los centros y que el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.



# LOS PRINCIPIOS DE LA PROTECCION DE DATOS:

## Derechos de los afectados

Cualquier persona podrá ejercer el derecho de acceso a sus datos, podrá rectificarlos cuando sean inexactos, cancelarlos (cuando la Ley lo permita) y oponerse al tratamiento de los mismos.

Todas estas solicitudes de ejercicio de dº que se reciban en la empresa deberán ser **inmediatamente** notificadas a la dirección, para que pueda atenderlas con la mayor celeridad posible.



# PLAZOS DE RESOLUCIÓN DE DERECHOS

- Dº DE ACCESO: PLAZO MÁXIMO DE **UN MES** A CONTAR DESDE LA RECEPCIÓN DE LA SOLICITUD.
- Dº DE RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN: PLAZO MÁXIMO DE **DIEZ DÍAS** A CONTAR DESDE LA RECEPCIÓN DE LA SOLICITUD.



# DERECHOS DE ACCESO

Es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.



El afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta:

- a. Visualización en pantalla.
- b. Escrito, copia o fotocopia remitida por correo, certificado o no.
- c. Telecopia.
- d. Correo electrónico u otros sistemas de comunicaciones electrónicas.
- e. Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.



# DENEGACIÓN DEL D° DE ACCESO

- Cuando el derecho ya **se haya ejercitado en los doce meses anteriores a la solicitud**, salvo que se acredite un interés legítimo al efecto.
- En los supuestos en que así lo prevea una **Ley o una norma de derecho comunitario de aplicación directa** o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.



# DERECHOS DE RECTIFICACIÓN

Es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.



# DERECHOS DE CANCELACIÓN

El ejercicio de este dº dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.



# DENEGACIÓN DEL Dº DE RECTIFICACIÓN Y CANCELACIÓN

La cancelación no procederá cuando los datos de carácter personal **deban ser conservados** durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.



# DERECHOS DE OPOSICIÓN

Es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo. Supuestos:

- a. Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.
- b. Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial,
- c. Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.



# MEDIDAS DE SEGURIDAD DE LOS DATOS

Las empresas, como responsables de los ficheros donde se ubican los datos de los usuarios, están obligadas a adoptar ***“las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural”*** (artículo 9 LOPD)



Las mencionadas medidas de seguridad deben quedar establecidas en el **Documento de Seguridad** que la empresa deberá elaborar, implementar y mantener actualizado; este documento deber ser accesible por el personal con acceso a datos, que resulta obligado por su contenido, así como estar a disposición de cualquier inspección que lo requiera.



# NIVELES DE SEGURIDAD PARA LOS DATOS

- **Nivel Básico:**
  - Datos personales, sin ninguna consideración específica. Por ejemplo: nombre, dirección, teléfono, etc...
- **Nivel Medio:**
  - Datos relativos a infracciones penales o administrativas.
  - Datos de carácter personal que permitan realizar una evaluación de la personalidad de un individuo.
- **Nivel Alto:**
  - Datos relacionados con la ideología, religión, raza, vida sexual.
  - Datos recabados con fines policiales pero sin consentimiento previo.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS:**

## **Identificación y autenticación**

- Todo usuario tendrá asignado un código de usuario y contraseña único y secreto a la aplicación o al sistema operativo formado por caracteres alfanuméricos.
- Se debe asegurar la confidencialidad e integridad de las contraseñas de los usuarios



Queda totalmente prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento de la dirección del centro con el fin de que se le asigne una nueva clave .



- Se deberá cambiar periódicamente la contraseña, sustituyéndola por otra distinta a las utilizadas anteriormente.
- Se evitarán nombres comunes fácilmente deducibles, números de matrículas de vehículos, teléfonos, nombres de familiares, amigos, etc. y derivados del nombre de usuario como permutaciones o cambio de orden de las letras, repeticiones de un único carácter... Constará como mínimo de 6 caracteres.
- No se accederá al sistema utilizando el identificador y la contraseña de otro usuario. Las responsabilidades de cualquier acceso realizado utilizando un identificador determinado, recaerán sobre el usuario al que se asignó.



- No se guardará la contraseña por escrito en ningún documento, ni en documentos electrónicos legibles.
- Los usuarios son responsables de la confidencialidad de sus contraseñas. En el caso de pérdida, olvido o sospecha de conocimiento por terceros de su contraseña se notificará a la dirección del centro.
- Las cuentas de acceso a los sistemas de información estarán ligadas a la identidad de la persona y no podrán ser compartidas, todo aquel usuario que intente acceder al sistema deberá identificarse de forma inequívoca y personalizada.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS: Control de acceso**

- Deben asociarse perfiles a los usuarios. Cada perfil accederá a unos datos y operaciones determinados.
- Se deben establecer mecanismos para la administración de perfiles de cada usuario.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS: Registro de accesos**

- Debe existir un log con datos detallados
  - Usuario
  - Fecha y hora
  - Fichero accedido
  - Tipo de acceso
  - Acceso autorizado o denegado

Para accesos autorizados: registros accedidos

- Los datos de este registro de accesos deben guardarse por un período mínimo de dos años.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS:**

## **Sistemas de información**

- Cuando un usuario tenga que abandonar su puesto de trabajo cerrará o bloqueará su sesión en el ordenador, además todos los ordenadores tendrán activado un protector de pantalla o cualquier otro sistema que impida la utilización del sistema si transcurrieran diez minutos sin que se realice ninguna operación, así como cerrará con llave la dependencia donde se encuentre el mismo.
- Los usuarios tendrán prohibida la instalación de software o demás productos informáticos en los ordenadores, sin autorización expresa, así mismo tendrán prohibido utilizar los recursos del sistema de información a los que tenga acceso para uso privado o para cualquier otra finalidad diferente de la estrictamente laboral.



- Se deben extremar las precauciones en aquellos sistemas de información en que se utilicen conexiones a Internet, para evitar ataques a los sistemas y minimizar la posibilidad de que se produzcan fugas de información, para ello se deben tener activados los “firewall”, antivirus, y adoptar toda medida adicional de protección que se considere conveniente.
- No se podrán introducir equipos informáticos de fuera de la empresa, conectarlos a la red corporativa y descargarse ficheros en los mismos, salvo autorización expresa de la entidad y deberá recogerse expresamente.



- Las pantallas, impresoras, fax, u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen una confidencialidad, el usuario en todo momento deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos del Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS:**

## **Confidencialidad de la información**

Si un usuario, por motivos directamente relacionados con el puesto de trabajo entra en posesión de información confidencial bajo cualquier tipo de soporte, se entiende que dicha posesión es **estrictamente temporal**, con obligación de secreto y sin que ello le irroque derecho alguno de posesión, o titularidad o copia sobre la referida información y siempre estará autorizada por la dirección del centro. Se deberán devolver dichos materiales a la empresa inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación laboral. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin consentimiento del centro podrá conllevar una responsabilidad.



- Cada usuario será responsable de la información que incorpore o modifique en la base de datos de la empresa.
- Los usuarios únicamente tendrán acceso a aquellos datos y recursos que precisen para el desarrollo de sus funciones.



# NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS:

## Gestión de soportes

**SOPORTE:** soporte físico que permite el almacenar o grabar datos (CD, DVD, PEN drive, disco duro externo...)

- La creación y salida de soportes con datos personales fuera de las dependencias de los centros deberá ser **expresamente autorizada** por la dirección de la empresa y deberán contener alguna **medida de seguridad** para impedir que dicha información pueda ser accesible a terceros no autorizados.
- Los soportes se almacenarán en lugar seguro.
- Cualquier soporte que haya contenido datos personales y se deseche, será destruido físicamente de forma que la información que contenía no pueda recuperarse.



- En caso de retirarse definitivamente los ordenadores personales de la empresa deberá procederse a la reinicialización de los discos internos de éstos, borrando todas las bases de datos de carácter personal, utilizando métodos que aseguren la imposibilidad de recuperación.
- Todos los documentos de papel de impresora con datos personales que se desechen serán destruidos, asegurándose que sea imposible su recomposición (ej. destructora de papel)
- Las labores de mantenimiento de los equipos informáticos de la empresa se efectuarán dentro de los locales del mismo, si ello no fuera posible la empresa se deberá asegurar que estos equipos no tienen datos personales, si no pudiera procederse a dicha operación, se habilitarán las medidas oportunas para preservar dicha información.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS:**

## **Copias de seguridad**

- Se deberán realizar copias de seguridad de los datos informatizados **al menos una vez a la semana**.
- Dicha copia de seguridad se realizará **fuera del equipo** del cual se pretende realizar una duplicidad de datos, nunca se almacenará en el mismo ordenador.
- Se deberá mantener copia de seguridad de la información en un **lugar diferente** del que se encuentren los equipos.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS: Gestión de incidencias**

**INCIDENCIA:** Cualquier incumplimiento de la normativa así como cualquier anomalía que pueda afectar a la seguridad de los datos de carácter personal de la empresa.

Constituye obligación de todo el personal de la empresa la notificación a la dirección de las incidencias de seguridad de acontezcan respecto a los recursos protegidos a la mayor brevedad posible.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS: Pruebas**

Las pruebas de los ficheros en los cuales se contengan datos personales, siendo al menos el nivel de seguridad de los datos de nivel medio, deben realizarse con datos ficticios.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS: Transmisión de datos**

Cualquier transmisión de datos debe realizarse mediante cifrado o equivalente, lo que implica, que la aplicación web debe funcionar como mínimo bajo protocolo https.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS:**

## **Tratamiento de datos por terceros**

Cualquier tratamiento de datos realizado por personal externo deberá estar regulado en un **contrato** en el que se estipularán las condiciones que regirán el acceso o tratamiento de los ficheros de la empresa.

El encargado del tratamiento sólo tratará los datos necesarios para la prestación de sus servicios, siendo responsabilidad de la empresa como Responsable del Fichero, vigilar que los datos **no sean excesivos**.



# EJEMPLOS DE PRESTACIONES DE SERVICIOS EN LAS EMPRESAS:

- Gestorías, asesorías jurídicas, despachos profesionales de asesores, abogados, economistas, contables, etc., encargados del tratamiento de los ficheros de PERSONAL y CONTABILIDAD.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS:**

## **Ficheros en papel**

- Los ficheros en soporte papel deberán ser almacenados, **bajo llave**, en un lugar específico destinado a los mismos.
- El acceso a los ficheros en papel deberá estar **autorizado por la empresa** y se limitará únicamente a aquellas personas que lo necesiten para el cumplimiento de sus funciones.
- A cada persona autorizada se le asignará una llave específica por la empresa que permitirá el acceso únicamente al lugar de almacenamiento de ficheros en soporte papel con acceso autorizado.
- Salvo que haya una persona autorizada presente en el lugar de almacenamiento, éste deberá mantenerse cerrado bajo llave.



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS:**

## **Política de uso de Internet**

Internet es un gran recurso potencial que permite acceder a información técnica especializada y mejorar y agilizar las comunicaciones, sin embargo una vez los datos salen de un ordenador, se desconoce la ruta que éstos siguen hacia su destino, en qué puntos intermedios se almacenan y quién puede acceder a ellos, copiarlos, modificarlos y utilizarlos para una finalidad diferente de aquella para la cual los envió.

Al no tratarse de una red de trabajo privada y segura, se debe realizar un **uso prudente** del mismo con fines laborales, poniendo límites y estableciendo controles de acceso y utilización de Internet.



Para evitar virus informáticos y componentes maliciosos que puedan dañar los sistemas o violar la confidencialidad de la información de la empresa, no se podrán utilizar chats o foros similares ni descargar o instalar cualquier archivo ejecutable o programa en la red de la empresa, **sin autorización expresa** de la dirección, quien aprobará o denegará su instalación una vez evaluada su utilidad para los fines relacionados con la entidad.

**Se prohíbe el uso de Internet de forma no ética, abusiva o inapropiada** y podrá ser causa de acción disciplinaria o despido. Ejemplos de usos inapropiados serían: la violación de cualquier ley de jurisdicción local, acceso o descarga de cualquier material de naturaleza ofensiva o sexual, juegos, comentarios o propuestas indecentes, enviar o descargar software comercial o cualquier otro material que viole los derechos de autor, interferencias intencionadas con el proceso de seguridad normal del centro, propagación deliberada de cualquier virus informático...



# **NORMAS ENCAMINADAS A GARANTIZAR LAS MEDIDAS DE SEGURIDAD DE LOS DATOS:**

## **Uso del correo electrónico**

- El e-mail es un recurso laboral que la empresa pone a disposición de los empleados para agilizar su gestión y debe ser utilizado únicamente con estos fines.
- No se podrá usar el sistema de e-mail de la empresa para actividades o negocios privados, o con propósitos de entretenimiento y diversión.
- Se debe extremar la precaución cuando se reciba un e-mail no deseado y bajo ninguna circunstancia se abrirán los archivos adjuntos.
- Cuando se dirija un mismo correo electrónico a más de un destinatario se deberá utilizar la herramienta de copia oculta (CCO) para garantizar la confidencialidad de las direcciones de correo.



# CONSECUENCIAS DEL INCUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD

Las actuaciones contrarias a lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en el RD 1720/2007 y demás disposiciones legales vigentes, podrían ocasionar una gran **violación de las libertades públicas y los derechos fundamentales de los titulares** de tales datos, lo cual es castigado por la ley con severas sanciones pecuniarias para los responsables de los ficheros desde los 900 hasta los 600.000 €uros, así como establece a los titulares de los datos personales afectados el derecho a una **indemnización** por los daños o lesiones sufridos en sus bienes o derechos.

Las sanciones e indemnizaciones impuestas a la empresa como consecuencia del incumplimiento, deliberado o negligente, por parte de un usuario de cualquier norma u obligación establecida en la ley, podrán ser repetidas contra el usuario infractor.



# AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



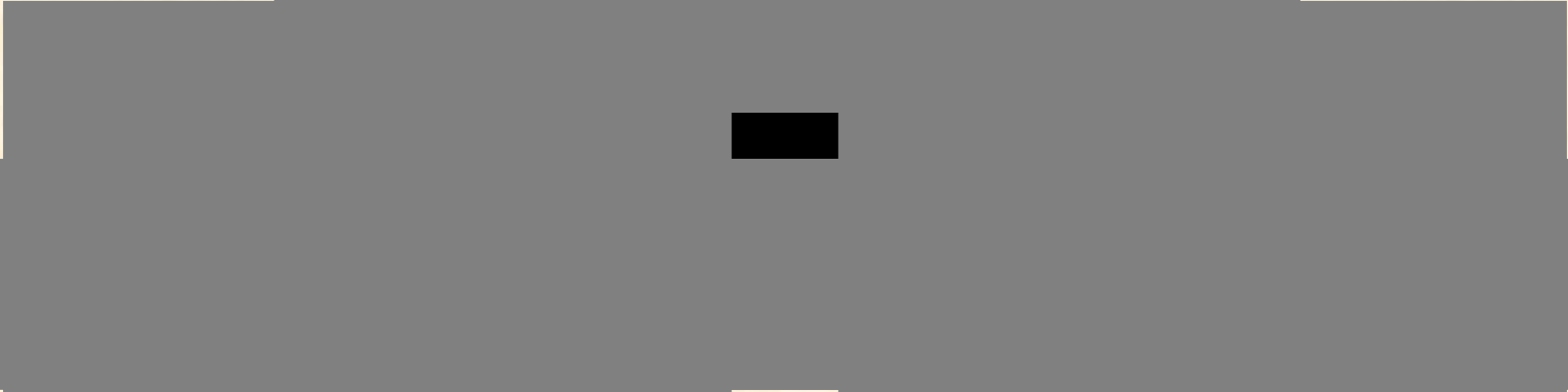
**PROTECTION REPORT S.L.**  
ESPECIALISTAS EN PROTECCIÓN DE DATOS

# FUNCIONES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

- 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 los datos
- Emitir las **autorizaciones** previstas en la Ley o en sus disposiciones reglamentarias.
- Dictar las **instrucciones** precisas para adecuar los tratamientos a los principios de la LOPD.
- Atender las **peticiones y reclamaciones** de las personas afectadas.
- **Informar** a las personas de sus derechos en materia de tratamiento de los datos de carácter personal.
- Requerir a los responsables y los encargados de los tratamientos, la **adopción de las medidas necesarias** para la adecuación del tratamiento de datos a las disposiciones de la LOPD y ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.
- Ejercer la **potestad sancionadora**.
- Informar los proyectos de **disposiciones generales** que desarrollen la LOPD.
- Recabar de los responsables de los ficheros ,ayuda e información necesaria para el desempeño de sus funciones.
- Velar por la **publicidad** de la existencia de los ficheros de datos de carácter personal.
- Redactar una **memoria anual** y remitirla al Ministerio de Justicia.
- Ejercer el **control y autorizaciones** necesarios en relación con los **movimientos internacionales** de datos, y cooperación internacional en materia de protección de datos personales.
- Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la **recogida de datos estadísticos** y al secreto estadístico.



# AGENCIA DE PROTECCION DE DATOS



# AGENCIA ESPAÑOLA DE PROTECCION DE DATOS

## SANCIONES

### INFRACCIONES LEVES

Multa de 900  
a 40.000 €uros

### INFRACCIONES GRAVES

Multa de 40.001  
a 300.000 €uros

### INFRACCIONES MUY GRAVES

Multa de 301.000  
a 600.000 €uros



- Leves

- **No atender**, por motivos formales, la solicitud del interesado de **rectificación o cancelación** de los datos personales objeto de tratamiento cuando legalmente proceda.
- No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
- **No solicitar la inscripción del fichero** de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
- Proceder a la **recogida de datos de carácter personal** de los propios afectados **sin proporcionarles la información que la LOPD determina**.
- **Incumplir el deber de secreto profesional**, salvo que constituya **infracción grave**.



- **Graves**
- Proceder a la **creación de ficheros** de titularidad privada o iniciar la **recogida de datos** de carácter personal para los mismos con **finalidades distintas** de las que constituyan el objeto legítimo de la empresa o entidad.
- Proceder a la **recogida de datos** de carácter personal de los afectados, cuando éste sea exigible **sin recabar el consentimiento expreso**
- Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la LOPD o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo.
- Mantener los **ficheros, locales, programas o equipos** que contengan datos de carácter personal **sin las debidas condiciones de seguridad** previstas por vía reglamentaria.
- **Incumplir el deber legal de información**, cuando los datos hayan sido recabados de persona distinta del afectado.



- **Muy graves**
  - La recogida de datos en forma **engañosa y fraudulenta**.
  - La **comunicación o la cesión de los datos** de carácter personal, **fuera de los casos permitidos**.
  - **Recoger y tratar los datos de carácter personal** especialmente protegidos sin el consentimiento expreso del afectado.
  - La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.
  - **Tratar los datos de carácter personal de forma ilegítima** o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.



# ¿POR QUÉ ADAPTAR LA WEB A LA LOPD?

- a) Respeto a la legalidad vigente, tanto por el espíritu de cumplir como para evitar las sanciones económicas derivadas de sanciones de la AEPD por incumplimiento de la LOPD.
  
- b) Mejorar la imagen de cara a potenciales clientes, infundiéndoles confianza en la marca o empresa y en particular, entre otros objetivos, en el comercio electrónico a través de la web de la empresa.



- En la web debería existir un enlace al “**Aviso legal**”, en el que se recogieran las obligaciones básicas dispuestas por la LSSI, como por ejemplo:
- Objeto del servicio proporcionado por la web.
- Responsabilidad del prestador del servicio.
- Propiedad intelectual e industrial.



También debería existir un enlace para acceder a la **“Política de Privacidad”** que siga el sitio web, indicando entre otros aspectos:

- El consentimiento expreso por parte del usuario para el tratamiento de sus datos.
- Autorización o no para la cesión de dichos datos a terceros.
- Informar al usuario de sus derechos de acceso, rectificación, cancelación, información y oposición.
- Otros: uso de cookies por parte de la aplicación web, uso de http, informar al usuario que se almacenará su dirección ip, etc....



# QUIENES SOMOS

Si en la web simplemente se hace una descripción genérica de la empresa y los servicios que prestan, sólo debe incluir una cláusula de **política general de privacidad** de la web.

Si incluye los nombres de determinados miembros de la empresa, incluso su fotografía o parte de su currículum (por ejemplo, sus estudios o los premios que han recibido), entonces obligatoriamente deberá haber solicitado el consentimiento expreso de cada uno de ellos para aparecer en la web, y haberles informado de su derecho a revocar ese consentimiento en cualquier momento y cómo y ante quién deben hacerlo.



# NUESTRA EMPRESA

Si va a difundir imágenes de sus instalaciones o centros de trabajo –tanto en fotografías como en vídeos- preste cuidado si aparecen en ellas trabajadores. Si las imágenes permiten identificar a las personas, o llegar a deducir su identidad a partir de algunos elementos, se les aplica la normativa de protección de datos, lo que significa que necesitará el consentimiento e información de los afectados. Además, si las imágenes van a ser libremente accesibles en internet, es recomendable que establezca políticas de privacidad, fijando condiciones de uso para terceros. Si en las imágenes aparecen trabajadores pero éstos no son identificables, entonces no se aplica la LOPD.



# ENVIENOS SU CURRICULUM

Los currículums contienen gran cantidad de datos de carácter personal, en muchos casos de nivel medio o alto. Por lo tanto, si su empresa invita en su web a los visitantes a enviar sus currículums o bien incluye un formulario para que sea cumplimentado con este mismo fin, debe informar a los candidatos de lo que va a hacer con esa información (es decir, incorporarla a un fichero con la finalidad de realizar procesos de selección), quién es el titular del fichero y cuáles son los derechos de los candidatos y cómo pueden ejercerlos. Por lo tanto, deberá incluir una cláusula de información y consentimiento que debe ser leída y aceptada para poder enviar el currículum.



# BOLETIN DE NOTICIAS O NEWSLETTER

Se ofrece al visitante que sus datos personales (incluso si sólo es una dirección de e-mail) sean agregados a una lista de distribución. Aunque los datos que se le soliciten sean mínimos, debe incluir una cláusula de información y consentimiento.

Además para realizar dichos envíos publicitarios se deberá cumplir con los requisitos de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).

Si quienes se van a suscribir al boletín son **empresas**, la LOPD se aplicará -o no- según el tipo de información que se recoja.



# CONTACTE CON NOSOTROS

Su web no debe aceptar el envío y recepción de estos formularios sin añadir la correspondiente cláusula de información y consentimiento, incluso si quien contacta con su empresa sólo va a proporcionarle datos personales elementales (por ejemplo nombre, apellido y correo electrónico).

La LOPD sanciona el tratamiento de datos personales sin cumplir con los principios de información y consentimiento -aunque sean básicos, pocos y se limiten a nombre, apellido y correo electrónico con fuertes sanciones que pueden alcanzar fácilmente los 300.000 euros, o incluso los 600.000 euros.



## ENVIAR A UN AMIGO

Si el visitante decide enviar información de la web a otra persona pero su empresa no va a quedarse con los datos del destinatario, no tiene que tener ninguna precaución con este procedimiento, puesto que no supone cesión de datos. Pero en el caso de que el envío incluya la comunicación de datos personales de ese “amigo” a su empresa, el titular de la web (es decir, su empresa), no puede quedarse sin más con éstos sin el consentimiento informado del titular de los datos (es decir, del “amigo”). Y más aún si el archivo de estos datos de “amigos” tiene un fin comercial.



# ENCUESTA

Se suele utilizar para recabar información sobre clientes y clientes potenciales.

Se debe incorporar a la encuesta una cláusula de información y consentimiento que debe aceptar quien responda a ella, es necesario cumplir con otro principio de la LOPD: la calidad de los datos, es decir, no se permite recoger cualquier tipo de datos, sino sólo aquellos que sean relevantes para la finalidad que se pretende, además en la clausula deberá especificarse si todas las preguntas son obligatorias o sólo algunas (ej. si se pregunta por el diseño de la web, no tendría sentido preguntar por profesión, aficiones o opinión sobre diferentes temas de actualidad del encuestado.



# TIENDA ON LINE

Los requisitos que tendrá que tener su web dependerán de:

- Si sólo se pueden hacer pedidos a través de la web (pero no pagarlos): simplemente deberá respetar las normas generales de información y consentimiento.
- Si también es posible efectuar el pago online: habrá que añadir una pasarela de pago seguro y acorde con la LOPD y la LSSI.



# DESCARGAS GRATIS

Depende de lo que su empresa quiera solicitar a cambio de descargarse algo. Si, por ejemplo, se trata de una demo de una nueva aplicación y hacerlo no requiere rellenar un formulario o no se rastrea la dirección del usuario, no se aplica la LOPD. En el caso de que se haga, deberá cumplir las mismas pautas indicadas anteriormente: derecho de información, finalidades previstas de uso, calidad de los datos respecto a las finalidades legítimas, consentimiento y ejercicio de derechos de acceso, rectificación, cancelación y oposición.



# PARTICIPAR EN UN CONCURSO

Al recoger los datos se deben indicar de manera muy precisa los términos y condiciones de participación del concurso y, sobre todo, si van a ser utilizados para otros fines.

En muchos casos el concurso será el anzuelo para captar un número significativo de direcciones y usarlas para fines publicitarios futuros, algo que no podrá hacer sin el consentimiento expreso de los participantes, puesto que, como regla general, si no le dieran el permiso para ello, la empresa deberá cancelar o destruir esos datos cuando dejen de ser necesarios, es decir, cuando acabe el concurso (si bien tendrá que mantenerlos bloqueados para hacer frente a posibles reclamaciones).



En el caso de que la base de datos que se genere con el concurso vaya a ser cedida a otra empresa o que su gestión se subcontrate a otra empresa, tendrá igualmente que indicarlo y obtener autorización expresa de los participantes, así como establecer con el tercero un contrato de prestación de servicios o de cesión, según el caso.



# ALOJAMIENTO WEB

En ocasiones se contrata el alojamiento de la página web con una empresa especializada, por lo que debemos asegurarnos de que los servidores se encuentran en España, pues de lo contrario todos los datos de su empresa incorporados en la web estarán alojados de hecho en el extranjero y tendrán que ser sometidos a las normas de transferencia internacional de datos.



Igualmente, si se va a producir acceso a datos personales por parte de la empresa de alojamiento, tendrá que establecer en un contrato las obligaciones de confidencialidad, prestaciones de servicios y responsabilidad de cada una de las empresas.

Lo mismo ocurriría si en su web corporativa participa una empresa de desarrollo de software o de mantenimiento informático.



# IMÁGENES EN LA WEB

- **Obligación** de cumplir con lo dispuesto por la LOPD cuando se trate de **personas identificadas o identificables**.
- Es necesario el **consentimiento expreso** de los sujetos que aparezcan en las imágenes.
- Debe aparecer **un aviso en las cámaras** que recojan imágenes que vayan a publicarse en la web.
- Si se trata de **cámaras** que pueden accederse **on-line**, dicho **acceso debe estar protegido**, al menos, mediante un mecanismo de identificación con usuario y contraseña.



# MENORES Y USO DE LA WEB

- En caso de **menores de 14 años**, es necesario el **consentimiento expreso** de sus padres o tutores.
- Si se trata de **un sujeto de 14 años o más**, dicho consentimiento no es necesario y pueden **consentir por sí mismos**.



- En todo caso, sería **recomendable** que una web destinada al uso por parte de menores contemplara:
- Un filtro de entrada, no permitiendo realizar reintentos en la misma sesión, tanto para realizar el registro como para identificarse.
- La no petición de datos relativos al entorno del menor, salvo para entrar en contacto o pedir autorización a sus padres o tutores.
- Una política de privacidad y uso de datos más clara y sencilla de lo habitual.



# BLOGS

Hay que considerar aspectos relacionados con los comentarios que pueden realizar a las entradas o post del blog:

- **Como usuarios de un blog**, no se deberían realizar comentarios en los que se recojan datos personales protegidos por la LOPD y no provenientes de fuentes públicas.
- Los **administradores de los blogs** deben moderar los comentarios, retirando aquellos que no cumplan con lo anterior.



# REDES SOCIALES

Las redes sociales online son servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado.



Los usuarios facilitan una serie de datos de carácter personal al inscribirse en estos portales que deben ser convenientemente protegidos conforme a la legislación española.

En unos casos, además, los datos son sensibles en cierta medida debido a la edad de los participantes (redes de ocio) y en otros debido a los datos de carácter económico (redes de contenido profesional),



Las redes sociales también deben ajustarse a todo lo anteriormente tratado en cuanto a:

- Existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información que introduzca en su perfil.
- Posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- Identidad y dirección del responsable del tratamiento de sus datos de carácter personal.



Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, la LOPD le obliga a designar, salvo que tales medios se utilicen con fines de trámite, un representante en España.

Esto sólo suele cumplirse por una pequeña parte de estas redes sociales extranjeras.



# ¿QUÉ LEGISLACIÓN ES LA APLICABLE EN CASO DE INFRACCIÓN DE ALGÚN DERECHO DENTRO DEL USO DE LA RED SOCIAL?

Los titulares de las redes sociales son responsables del tratamiento de datos personales y, si están establecidos en algún Estado miembro de la Unión Europea o utilizan medios de tratamiento ubicados en la misma, deben cumplir la normativa europea –española si están establecidos en España –sobre protección de datos personales al utilizar medios ubicados dentro de la Unión Europea.



Los titulares de redes sociales que tienen su sede fuera la Unión Europea, según el artículo 4º de la Directiva 95/46/CE les será de aplicación las disposiciones adicionales aprobadas para la aplicación de la Directiva en todo tratamiento de datos cuando el responsable no esté establecido en la Unión Europea pero recurra, para el tratamiento de datos personales, a medios situados en el territorio de dicho Estado.



Los usuarios de estas redes deben tener la posibilidad de **acceder** a los datos registrados a fin de comprobar su exactitud y **rectificarlos** si son inexactos o incompletos, o si están desfasados, así como **oponerse** a los mismos y **cancelarlos** si así lo desean, porque resulten inadecuados o excesivos o en caso de solicitud de baja en la red social.



Aunque la LOPD no se aplica a los ficheros de personas físicas creados en el ejercicio de actividades exclusivamente personales o domésticas, los propios usuarios podrían ser considerados responsables de tratamiento de los datos que introducen (ej. caso de facilitar datos de amigos, publicación de fotografías...)



Así como la propia red social podría ser considerada también responsable al ser intermediaria, ya que es a través de la misma donde se publica la información y es quien está obligada a la cancelación de la misma en tanto en cuanto infrinja un derecho.





**PROTECTION REPORT S.L.**

ESPECIALISTAS EN PROTECCIÓN DE DATOS

**Atención al cliente 902 364585**

-Paseo del Violón, 8. Local - GRANADA

-Torneo Parque Empresarial, C/ Arquitectura, 4. Torre 10,  
Planta 6ª, Mod. 4 - SEVILLA

-Valle de Pinares Llanos, 8 B, 2º B - MADRID



**PROTECTION REPORT S.L.**

ESPECIALISTAS EN PROTECCIÓN DE DATOS



**PROTECTION REPORT S.L.**  
ESPECIALISTAS EN PROTECCIÓN DE DATOS