

LEY DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

En los últimos tiempos, cada vez más, se viene hablando mucho de la protección de datos de carácter personal. En este número vamos a intentar dar un repaso a los conceptos que tienen algo que ver con la Ley Orgánica de Protección de Datos (LOPD), ley de obligado cumplimiento para todas las empresas y por culpa de la cual, se están imponiendo cuantiosas sanciones a las empresas que no cumplen con ella.

La Ley Orgánica de Protección de Datos se creó con el fin de proteger al ciudadano (no a las empresas, que quedan excluidas de la misma) del abuso que algunas personas o empresas cometían con sus datos, vendiéndolos, alquilándolos o utilizándolos para otros usos distintos de para los que fueron recabados.

La Ley de Servicios de la Sociedad de la Información es una ley que amplía la Ley Orgánica de Protección de Datos, prolongándola al terreno de Internet, las páginas web y el mal uso del e-mail.

Recientemente ha habido cambios muy importantes, entre los que se cuenta el que el código penal condene, con penas de prisión de hasta 4 años, el uso indebido de datos sacados de una compañía de forma ilícita. Esto permite a las empresas protegerse de las malas prácticas de algunos empleados.

¿Qué es la LOPD?

Es la ley que se encarga de velar por los datos de las personas y de regular la comunicación y el intercambio de ficheros que contengan datos de personas.

Es importante decir que la ley es de 13 de diciembre de 1999 y que se establecieron tres fechas de entrada en vigor, la última de las cuales fue el 26 de junio de 2002, con lo que se trata de un hecho consolidado y que todas las empresas deben acatarla.

¿A quién va dirigida y cuál es su objetivo?

La ley tiene por objeto garantizar y proteger el tratamiento de los datos de carácter personal de las personas físicas y se tendrá que aplicar a aquellas empresas o particulares que se encuentren en territorio español y tengan ficheros físicos con datos de carácter personal.

Principios de la protección de datos

Los datos de carácter personal que se recojan sólo podrán utilizarse para el fin por el que se recogieron, no pudiéndose usar para otra cosa salvo consentimiento expreso del afectado. Si pasado un tiempo los datos que tenemos no coinciden con los verdaderos, deberemos corregirlos o cancelarlos de nuestra base de datos no pudiendo permanecer en ella datos inexactos.

Seguridad de los datos

La ley establece tres niveles de seguridad para los ficheros que contienen los datos de carácter personal, en función de la naturaleza de esos datos.

Todos los ficheros, sean sus datos de la naturaleza que sean, tienen que adoptar las medidas de seguridad básicas o de primer nivel, que consisten principalmente en el control de los accesos y la copia y traslado de los datos.

Aquellos ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros o cuando contengan datos suficientes que permitan obtener una evaluación de la personalidad del individuo, deberán garantizar, además, las medidas de nivel medio, que consisten principalmente en reforzar el control de los accesos y en realizar cada dos años una

auditoría interna o externa que compruebe las medidas de seguridad adoptadas y el cumplimiento de ellas.

Los ficheros que contengan datos relativos a la ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas, deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto. Estas medidas contemplan el cifrado de los datos cuando tengan que ser trasladados o desplazados de su ubicación controlada y en llevar un registro detallado de los accesos que se realizan a los datos, que deberá ser revisado y controlado por el responsable del fichero al menos una vez al mes.

En todos los casos, el responsable del fichero o tratamiento tendrá que elaborar un Documento de Seguridad, que recogerá las medidas de índole técnica y organizativa adoptadas para garantizar la seguridad de los datos, que serán de obligado cumplimiento para todo el personal con acceso a ellos.

DOCUMENTO DE SEGURIDAD

El Documento de Seguridad deberá contener y detallar, como mínimo, los siguientes aspectos:

- **Ámbito de aplicación del documento de seguridad:** En el caso de que haya más de un fichero o tratamiento a proteger, se podrá tener un único Documento de Seguridad o varios.
- **Medidas, normas, procedimientos, reglas y estándares** encaminados a garantizar el nivel de seguridad exigido.
- **Funciones y obligaciones del personal con acceso a los datos**
- **Estructura de los ficheros y descripción de los tratamientos** que se realizan con ellos
- **Procedimientos a seguir ante las incidencias**
- **Procedimientos para la realización de copias de respaldo y recuperación de los datos**
- **Medidas a adoptar para el transporte y la destrucción de los datos protegidos.**

Para los ficheros o tratamientos que exijan seguridad de nivel medio o alto, habrá que incluir en este documento también, la identificación del responsable de seguridad y los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento

El documento de seguridad deberá mantenerse actualizado en todo momento y será revisado siempre que se produzcan cambios relevantes en el sistema de información, es decir, cuando dicho cambio pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

DEFINICIONES

Datos de Carácter Personal: Cualquier información concerniente a personas físicas identificadas o identificables

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso

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.

Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

Encargado del tratamiento: Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero.

Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.

Fuentes accesibles al público: Aquellos ficheros cuya consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa o, sin más exigencia que, en su caso, el abono de una contraprestación. Tienen consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos (en los términos previstos por su normativa específica), los diarios y boletines oficiales, los medios de comunicación y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.

¿Qué hacer si recojo datos personales?

La ley nos indica que informemos de las siguientes cuestiones a todas las personas a las que les tomemos datos personales:

1. De la 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.
2. Del carácter obligatorio o voluntario de su respuesta a las preguntas que le sean planteadas
3. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos, si las hubiera.
4. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
5. De la identidad y dirección del responsable del tratamiento o en su caso de su representante.