GUÍA PRÁCTICA DE CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

1. INTRODUCCIÓN

El progresivo desarrollo de las técnicas de recogida y almacenamiento de datos implica múltiples posibilidades de reunir, almacenar, relacionar y transmitir todo tipo de información relativa a las personas.

Todo ello supone un potencial peligro para cualquier individuo, al proporcionar a terceros el conocimiento de hechos que pertenecen a la esfera privada de las personas.

Resulta, pues, necesario, establecer mecanismos legales que protejan al individuo de los riesgos que para su intimidad, honor y libertad se pueden derivar de la utilización de sus datos de carácter personal. La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, "LOPD") tiene como objeto la protección de los datos personales de los ciudadanos con dicho fin.

La presente guía práctica tiene como finalidad explicar brevemente el contenido de la LOPD y elaborar unas indicaciones prácticas que permitan a las empresas cumplir sus disposiciones normativas.

2. DEFINICIONES

La LOPD contiene una serie de definiciones legales, que analizamos a continuación:

A.- Datos de carácter personal: "cualquier información concerniente a personas físicas identificadas o identificables".

Son datos de carácter personal, por ejemplo, el nombre, apellidos, NIF, dirección, así como cualquier otro tipo de información que se encuentre vinculada a una persona.

Al hacerse expresa mención a las "*personas físicas*", la LOPD excluye de su ámbito de aplicación a las personas jurídicas (p.e. sociedades).

B.- 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".

C.- Fichero: "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

Estos ficheros pueden encontrarse en soporte informático (por ejemplo, un programa de ordenador) o en papel.

3. OBLIGACIONES QUE IMPONE LA LOPD A LAS EMPRESAS

La LOPD establece una serie de obligaciones:

3.1. Inscripción de ficheros

Es obligatorio inscribir los ficheros de datos de carácter personal en el Registro General de la Agencia Española de Protección de Datos.

Además, si se modificase la estructura o características de sus bases de datos, debe solicitar a la Agencia Española de Protección de Datos la modificación de la inscripción de sus ficheros.

Por último, en el momento de cese de la actividad, deberán darse de baja en la Agencia Española de Protección de Datos la inscripción de sus ficheros.

3.2. Calidad de los datos

La recogida de datos para su tratamiento y posterior utilización únicamente está permitida, de acuerdo con la LOPD, cuando los datos "*sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y*

legítimas para las que se hayan obtenido". Igualmente, los datos de carácter personal "*serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados"*.

3.3. Seguridad de los datos

De acuerdo con lo establecido en la LOPD, las empresas deberán adoptar las medidas necesarias para mantener la seguridad de los datos personales, evitando su alteración, pérdida, tratamiento o acceso no autorizado, tanto si se encuentran en soportes informáticos como si se hallan en documentos en papel.

Esta obligación se traduce en la práctica en el cumplimiento de una serie de medidas de seguridad, que han de hacerse constar por escrito en lo que se denomina "Documento de Seguridad".

El Documento de Seguridad debe mantenerse actualizado, por lo que debe ser periódicamente revisado por la propia tienda.

3.4. Deber de secreto

La LOPD señala que "el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."

El deber de secreto incumbe tanto al empresario como al personal a su servicio. Por ello, es conveniente que los empleados firmen una cláusula de confidencialidad.

3.5. Acceso a datos por cuenta de terceros

En el desarrollo de la actividad de una empresa suelen existir terceras personas o empresas que prestan servicios a la tienda y que, para ello, tienen acceso a los datos de carácter personal de la misma.

Los tratamientos de datos de carácter personal por cuenta de terceros deben estar regulados en un contrato escrito.

3.6. Información en la recogida de datos y consentimiento del afectado

Al obtener datos personales (de clientes, empleados, etc.) existe la obligación de informar al interesado de que dichos datos se incorporarán a un fichero o tratamiento, así como obtener el consentimiento expreso de éste.

Este consentimiento se obtendrá del modo siguiente:

- Datos de clientes: El consentimiento del cliente para el tratamiento de sus datos se presta mediante la firma del documento en el que se incorpore la cláusula de información antes referida. Es fundamental que el documento en el que se incluya la cláusula sea siempre firmado por el cliente y que la empresa conserve el original con la firma y entregue al interesado una copia.

- Datos de empleados: El consentimiento de los empleados para el tratamiento de sus datos personales se manifiesta por la firma del documento en el que se incluye la cláusula de información antes referida.

4. COMUNICACIÓN DE DATOS A TERCEROS

La comunicación a terceros de los datos personales de los ficheros de las empresas sólo puede realizarse cuando se recabe previamente la autorización del titular de los datos, salvo disposición legal expresa.

Fuera de estos casos, no se deben revelar datos a tercero, salvo que la revelación de datos sea precisa para una prestación de servicios y siempre previa celebración de contrato escrito de acceso a datos antes mencionado.

5. DERECHOS DE ACCESO, RECTIFICACIÓN Y CANCELACIÓN

En virtud de la LOPD, los interesados disponen de los derechos de acceso, rectificación, cancelación y oposición, que pueden hacer valer ante la empresa.

5.1. Derecho de acceso.

El derecho de acceso es la facultad de todo interesado de solicitar y obtener información acerca de sus datos de carácter personal que estén sometidos a tratamiento, el origen de dichos datos y las comunicaciones realizadas o que se prevean hacer de los mismos.

5.2. Derecho de cancelación.

La cancelación es el proceso de borrado de datos que se debe realizar en los supuestos en que los datos del fichero resulten inadecuados o excesivos con relación a su finalidad, así como cuando dejen de ser necesarios para el fin para el que fueron recabados.

5.3. Derechos de rectificación.

La rectificación es un proceso a aplicar en aquellos supuestos en los que existan datos erróneos o inexactos en los ficheros. A diferencia de la cancelación, no consiste en el borrado o destrucción física de los datos, sino únicamente en la sustitución de los mismos por aquellos que sean correctos.

5.4. Derecho de oposición.

La oposición implica la negativa del interesado a que sus datos sean utilizados con determinada finalidad, entre las varias para las que fueron entregados.

Dicha petición implicará que los datos personales podrán usarse para los fines permitidos pero no podrán utilizarse con las finalidades que el interesado no desee.

6.- INFRACCIONES Y SANCIONES

La LOPD establece un riguroso régimen de infracciones y sanciones en caso de incumplimiento.

El órgano administrativo competente para el control del cumplimiento de esta normativa e imponer sanciones por

incumplimiento es la Agencia Española de Protección de Datos (AEPD).

Las infracciones que prevé la Ley se clasifican en leves, graves y muy graves. Las primeras pueden ser sancionadas con multa de 600 a 60.000 €, las segundas de 60.001 a 300.000 € y las terceras con multa de 300.000 € a 600.000 €.

Ejemplos de infracciones leves son no notificar los ficheros con datos personales a la AEPD o no informar convenientemente a los interesados en el momento de recabar sus datos personales. De infracciones graves lo son tratar los datos personales sin consentimiento del interesado o no cumplir las medidas legales que garanticen la seguridad de los ficheros con datos personales. Ejemplo de infracción muy grave lo es comunicar datos a tercero sin consentimiento del interesado.