Obligaciones de la empresa en materia de Protección de Datos

Existe la falsa creencia de que sólo las empresas que desarrollan actividades relacionadas con las Nuevas Tecnologías están obligadas a cumplir las obligaciones que impone la **Ley de Protección de Datos** (Ley Orgánica 15/1999, de 13 de diciembre). Sin embargo hay que empezar recordando que esta ley es **de obligado cumplimiento para TODAS las personas físicas o jurídicas que posean datos de carácter personal de personas físicas**:

- **Afecta tanto a personas jurídicas** (empresas, asociaciones, fundaciones,etc.) **como a personas físicas** (particulares o autónomos) y a las Administraciones Públicas.
- Estarán sometidas siempre **que posean datos de carácter personal de personas físicas**. No se aplica por lo tanto a aquellas que sólo posean datos de personas jurídicas.

Incluso los particulares que no ejerzan actividades económicas podrían verse obligados a cumplir estas obligaciones. No obstante, la Ley excluye de las misma a los ficheros mantenidos por personas físicas en el ejercicio de «actividades exclusivamente personales o domésticas».

¿QUE SE ENTIENDE POR DATOS DE CARÁCTER PERSONAL?

Por dato de carácter personal se entiende cualquier información referida a **personas físicas** (no jurídicas) identificadas o identificables: Nombre y apellidos, dirección, teléfono, DNI, número de la seguridad social, fotografías, firmas, correos electrónicos, datos bancarios, edad y fecha de nacimiento, sexo, nacionalidad, etc. Es decir, **datos personales son todos aquellos que permiten identificar a una determinada persona**.

Normalmente, a la hora de mencionar estos datos se habla de **ficheros**, ya sean automatizados (en soporte informático) o no automatizados (en soporte físico o papel). Los ficheros son aquellas bases de datos que recogen de forma organizada los datos de carácter personal que tienen cierta relación entre si (una empresa puede tener fichero de

clientes, donde figuran los datos personales de los clientes, otro fichero de proveedores, donde figuran los datos personales de los proveedores, otro de curriculums, etc.)

Por ejemplo, a un fichero en excel con datos de clientes (nombre, apellidos, teléfono, email, etc.) le será de aplicación la ley y las obligaciones que vemos a continuación ya que se trata de datos de personas físicas; pero si tenemos otro fichero con datos de proveedores (nombre de empresa, cif, dirección, etc.) no le será de aplicación ya que son datos de personas jurídicas. Ahora bien, si en este último fichero hubiese datos de autónomos, sí sería de aplicación la ley ya que estos son personas físicas.

¿QUIEN ESTÁ OBLIGADO A CUMPLIR LA LEY?

La Ley distingue entre el **responsable** del fichero, es decir, el titular o propietario del mismo, y el **encargado del tratamiento** del fichero, que es aquel que está encargado de utilizar los datos por cuenta del anterior. Es posible que sólo exista el Responsable, que es el titular y el que hace uso de los datos directamente, pero también son típicos casos como los de las asesorías que se encargan de realizar las nóminas con los datos de los trabajadores facilitados por una empresa X.
En este caso **el Responsable del fichero es la empresa X y el encargo del tratamiento será la asesoría**.

En todo caso, es importante tener en cuenta que es el responsable o titular del fichero, la empresa X, la obligada a cumplir la gran mayoría de las obligaciones impuestas en la ley.

¿QUE TIPOS DE DATOS PUEDEN RECOGERSE?

El objetivo de la ley es la protección del derecho al honor y a la intimidad de las personas, por lo que, en función de la «sensibilidad» de los datos que se recojan, variarán los niveles de protección exigidos por la ley. Se distinguen tres niveles:

1. **Nivel alto**: se incluyen en este nivel los datos referidos a la ideologías políticas, afiliaciones sindicales, creencias religiosas, origen racial, datos sobre la salud o la vida sexual.

2. **Nivel medio**: se incluyen aquí los datos referidos a la comisión de infracciones administrativas o penales, servicios financieros, solvencia patrimonial o crédito (ficheros de morosos e impagados), datos en la Hacienda Pública, datos de los que se extraiga la personalidad de un sujeto (gustos, aficiones, estilo de vida, etc.)
3. **Nivel básico**: este nivel englobará el resto de datos; nombre y apellidos, dirección, teléfono, DNI, número de la seguridad social, fotografías, firmas, correos electrónicos, datos bancarios, edad y fecha de nacimiento, sexo, nacionalidad, etc.

¿CUALES SON LAS OBLIGACIONES QUE IMPONE LA LEY?

Por lo tanto, todas aquellas personas físicas o jurídicas que tengan alguno de estos datos, ya sea de clientes, usuarios o visitantes, empleados, proveedores, etc. ya sea **en soporte informático o en papel**, deben cumplir las obligaciones que resumimos brevemente a continuación:

Calidad de los datos

Los datos de carácter personal sólo se podrán recoger 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 no podrán usarse para **finalidades incompatibles** con aquellas para las que los datos hubieran sido recogidos. Deben **cancelarse o rectificarse** los datos inexactos y serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados.

Derecho de información en la recogida de datos

Cuando se utilicen formularios, cuestionarios u otros impresos para la recogida de datos figurarán en los mismos, **en forma claramente legible**, la siguiente información:

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 facultativo de su respuesta a las preguntas que les sean planteadas.

3. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
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.

No obstante, no será necesaria la información a que se refieren los números 2, 3 y 4 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Consentimiento del afectado

El tratamiento de los datos de carácter personal requerirá el **consentimiento inequívoco** del afectado, salvo que la ley disponga otra cosa. El consentimiento **podrá ser revocado** cuando exista causa justificada para ello.

Datos especialmente protegidos

Como decíamos anteriormente, los datos incluidos en el nivel alto y medio están especialmente protegidos, por lo que en caso de no ser absolutamente necesarios para el ejercicio de nuestra actividad, **es recomendable NO solicitarlos**. Así, por ejemplo, quedan prohibidos los ficheros creados con la finalidad «exclusiva de almacenar» datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual. Por otro lado, de acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias, por lo que cuando se proceda a recabar el consentimiento al tratamiento de estos datos se advertirá al interesado acerca de su derecho a no prestarlo.

Deber de secreto

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 incluso después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Comunicación o cesión de datos

Los datos de carácter personal sólo podrán ser comunicados o cedidos a un tercero para el cumplimiento de **fines directamente relacionados** con las funciones legítimas del cedente y del cesionario **con el previo consentimiento del interesado**. Por lo tanto, para ceder los datos personales, es necesario que se den los dos requisitos anteriores, incluido el consentimiento del interesado.

Respecto al consentimiento hay que tener en cuenta que:

- Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.
- El interesado puede revocarlo.

El consentimiento exigido en el apartado anterior no será preciso:

- Cuando la cesión está autorizada en una ley.
- Cuando se trate de datos recogidos de fuentes accesibles al público.
- Cuando 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. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.
- Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Acceso a los datos por cuenta de terceros (Encargo de tratamiento)

Como indicábamos anteriormente en el ejemplo de la asesoría, es posible que un tercero, diferente del Responsable del fichero, sea el que realice el tratamiento de los datos. En estos casos se exige que exista un **contrato de encargo de tratamiento** entre el Responsable (Empresa X) y el encargado del tratamiento (asesoría), en el que se indique la forma de tratar los datos y las medidas de seguridad a adoptar.

Derechos de las personas

Hay que tener en cuenta que las personas afectadas tienen los siguientes derechos:

- **Derecho de acceso**: Derecho a conocer toda la información referente a sus datos personales de los que dispone la empresa. Esta debe responder en el plazo máximo de 1 mes; si no lo hace así, el afectado podrá recurrir ante la Agencia de Protección de Datos.
- **Derecho de rectificación y modificación** de sus datos. La empresa tiene 10 días para hacer las modificaciones solicitadas. Transcurrido este plazo sin recibir respuesta o siendo esta insatisfactoria, puede recurrir ante la Agencia de Protección de Datos.
- **Derecho de cancelación** de sus datos, que la empresa debe eliminar salvo que por disposición legal deban conservarse.
- **Derecho de oposición**, negándose a que un tercero trate sus datos de carácter personal, salvo que exista disposición legal que obligue a su tratamiento.
-

Seguridad de los datos

El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán 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.

Hay que tener en cuenta que cuando los ficheros están en soporte informático, existe una regulación específica contenida en el Real Decreto 994/1999, que determina las medidas de seguridad a adoptar. Este Real Decreto exige que se redacte un **Documento de Seguridad** en el que se incluya:

1. Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
2. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
3. Funciones y obligaciones del personal.
4.
5. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
6. Procedimiento de notificación, gestión y respuesta ante las incidencias.

7. Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Cuando los datos recogidos pertenecen a los niveles medios o altos, las medidas de seguridad serán mayores (deberá nombrarse un responsable de seguridad, deberá someterse a una auditoría, deberá tener sistemas para identificar a los usuarios que accedan a los datos, sólo el personal autorizado podrá acceder a la información, deberán hacerse copias de seguridad, etc.)

Puede consultar una Guía de Seguridad y utilizar el modelo de Documento de Seguridad que facilita la Agencia de Protección de Datos.

Notificación de ficheros

El responsable o titular debe notificar los ficheros a la **Agencia de Protección de Datos** antes de su creación.

Lo que se comunica son los datos del titular de la base de datos, el nombre del fichero, su descripción, estructura, etc, pero NO se comunican los datos incluidos en los ficheros. P.e. Si vamos a crear un fichero llamado «*clientes*«, comunicaremos el nombre del fichero, su estructura, finalidad, efectos, etc … pero no los datos de nuestros clientes.

Esta notificación puede hacerse por Internet. Para ello, en la página de la Agencia de Protección de Datos tendremos que descargarnos un programa para la notificación de ficheros de titularidad privada. Una vez instalado cumplimentaremos todos los datos con la ayuda que presenta el programa. Una vez terminado, mediante la opción correspondiente, enviaremos los datos a la Agencia. Posteriormente, si no disponemos de firma electrónica, tendremos que **imprimir una hoja de solicitud que genera el programa y enviarla firmada a la Agencia de Protección de Datos.**Al cabo de un mes, aproximadamente, recibiremos contestación confirmándonos la inscripción del fichero.
Este proceso debe repetirse para cada uno de los ficheros que tengamos (de clientes, de proveedores, de trabajadores, etc.)

Por último aconsejamos que en caso de duda se deje en manos de un profesional (imprescindible cuando se manejan datos especialmente protegidos). Hay que tener en

cuenta que el incumplimiento de esta ley es todavía masivo, la ley es bastante estricta y las sanciones «muy» elevadas (de 600 a 600.000 euros).

Ejemplos reales:

- IMPONER a la entidad …… , por una infracción del artículo 21 de la LSSI, tipificada como leve en el artículo 38.4.d) de dicha norma, una multa de **3.000 euros** (Tres mil euros) de conformidad con lo establecido en el artículo 39.1 y 40 de la citada Ley … POR ENVIAR UN EMAIL CON FINES COMERCIALES NO AUTORIZADO.
- IMPONER al ……. ……..., por una infracción del artículo 11.1 de la LOPD, tipificada como muy grave en el artículo 44.4.b)de dicha norma, una multa de **300.506,05** (trescientas mil quinientos seis con cinco céntimos) de euros, de conformidad con lo establecido en el artículo 45.3 y 4 de la citada Ley Orgánica.
- IMPONER a la entidad ……. ……..., por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de **60.101,21** (sesenta mil ciento un euros con veintiún céntimos) de euros, de conformidad con lo establecido en el artículo 45.2 y 4 de la citada Ley Orgánica.
- IMPONER a la entidad ……., por una infracción del artículo 4.7 de la LOPD, tipificada como muy grave en el artículo 44.4.a) de dicha norma, una multa de **300.506,05** (trescientos mil quinientos seis euros con cinco céntimos) de conformidad con lo establecido en el artículo 45. 3 y 4 de la citada Ley Orgánica.