LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La **Ley Orgánica de Protección de datos** tiene como objeto el garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, especialmente de su honor e intimidad personal y familiar, en lo concerniente al tratamiento de sus datos personales.

La **LOPD** entiende por datos de carácter personal cualquier información sobre las personas físicas identificadas o identificables, tales como:

- Nombre y apellidos, DNI, dirección, datos bancarios, etc.
- Datos **especialmente sensibles**: ideología, religión o creencias, raza, salud, vida sexual, afiliación sindical, etc.

EL REGLAMENTO DE MEDIDAS DE SEGURIDAD (RD 994/1999, DE 11 DE JUNIO)

Este reglamento está asociado a la **LORTD** de 1995 y no a la **LOPD**, que es posterior, de modo que determina las medidas técnicas y organizativas mínimas que deben establecerse para la información de carácter personal sobre la que se realiza un tratamiento automatizado.

Establece tres niveles de seguridad:

- **Básico:** cualquier dato de tipo personal, nombre, DNI, dirección, etc.
- **Medio:** datos de comisión de infracciones penales y administrativas, Hacienda Pública, servicios financieros, ficheros de publicidad.
- **Alto:** datos sensibles como ideología, religión, raza, salud o vida sexual.

Los plazos máximos que marca la Ley para adaptar los ficheros son:

- 26 de diciembre de 1999, prorrogado a 26 de marzo de 2000: medidas de **nivel básico**.
- 26 de junio de 2000: medidas de **nivel medio**.
- 26 de junio de 2002: medidas de **nivel alto**.

LA AGENCIA DE PROTECCIÓN DE DATOS

La **Agencia de Protección de Datos** es un organismo oficial, creado con la finalidad de velar por el cumplimiento de la normativa sobre protección de datos personales informatizados y controlar su aplicación.

Centraliza el **registro de ficheros** con datos de carácter personal de todas las empresas que los hayan declarado.

Realiza **inspecciones en las empresas** a instancia de los afectados o de oficio.

Es competente para **instruir y resolver los expedientes sancionadores** por la comisión de las infracciones previstas en la ley:

- Infracción **leve**: multa de 600 a 60.000 euros
- Infracción **grave**: multa de 60.000 a 300.000 euros
- Infracción **muy grave**: multa de 300.000 a 600.000 euros

La División de Derecho de los Sistemas de Información de **ALCAZAR PATENTES & MARCAS**, realiza el proyecto de adaptación a la **Ley de Protección de Datos de Carácter Personal** a través de tres enfoques claramente diferenciados pero complementarios:

ENFOQUE ORGANIZATIVO

Realizando una definición de la estructura organizativa, funciones y procedimientos de su empresa para estar en disposición de cumplir escrupulosamente con las medidas dispuestas en la **LOPD**.

ENFOQUE INFORMÁTICO

Definiendo los niveles adecuados de confidencialidad, integridad y disponibilidad de la información custodiada por su empresa, mediante el diagnóstico de las medidas tecnológicas, de normas y procedimientos y de formación implantadas en los **Sistemas y Tecnologías de la Información** de la la empresa.

Desarrollando el **Documento de Seguridad** requerido en el Reglamento de Seguridad y cuyo contenido va a constituir la columna vertebral de las medidas de seguridad establecidas para los ficheros de datos de cualquier nivel. Dicho documento constará de los siguientes apartados:

- Ámbito de aplicación del documento.
- Medidas, Normas y Procedimientos garantizadores del nivel de seguridad exigido en el Reglamento.
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que tratan.
- Procedimientos de notificación , gestión y respuesta ante incidencias.
- Procedimientos de realización de copias de respaldo y recuperación de datos.

PRODUCTO FINAL

El producto final del trabajo a realizar por **ALCAZAR** consistirá en:

- Identificación de los ficheros físicos que contienen datos de carácter personal.
- Declaración de nuevos ficheros lógicos o modificación de los ya declarados en la APD.
- Informe de cumplimiento de la empresa con la normativa vigente en materia de protección de datos desde el punto de vista organizativo, jurídico e informático.
- Elaboración de un plan de acción de medidas a adoptar por la empresa para el cumplimiento de la normativa.
- Propuesta de formación y concienciación del personal.
- Elaboración del DOCUMENTO DE SEGURIDAD previsto en el Reglamento de Medidas de Seguridad.

RECIENTEMENTE SE HA PUBLICADO EL REAL DECRETO 1720/2007, DE 21 DE DICIEMBRE POR EL QUE SE APRUEBA EL REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL, que establece una serie de medidas de obligado cumplimiento para todos aquellos profesionales o empresas que traten datos de carácter personal, en el ejercicio de su actividad profesional, tanto en papel como en formato automatizado.

ALCAZAR, puede llevar a cabo la adecuación de su empresa a esa normativa e indicarle qué requisitos y qué procedimientos se han de seguir para cumplirla y para actuar ante las denuncias formuladas ante la Agencia de Protección de Datos, ofreciéndole soluciones en el ámbito jurídico, técnico y organizativo.

ALCAZAR le ofrece un servicio de asesoría global, dando solución tanto a las deficiencias de carácter jurídico como a las que le pudieran afectar en el plano técnico y organizativo.

El servicio comprende:

- Diagnóstico de la situación real y detección de posibles incumplimientos.
- Identificación de los ficheros existentes y del nivel de seguridad a implantar.
- Inscripción de los ficheros ante el Registro General de Protección de Datos.
- Redacción de contratos, cláusulas y formularios.
- Elaboración del Documento de Seguridad.

- Informe de adecuación y propuestas de implantación de las obligaciones técnicas y organizativas precisas para cumplir la normativa.

- **AUDITORIA** bianual.

La normativa vigente establece la obligación de velar continuamente por el cumplimiento de las medidas y procedimientos adoptados y exige llevar a cabo una Auditoría, al menos cada dos años, a fin de verificar el cumplimiento de esta normativa.

- **CONSULTORÍA Y AUDITORÍA WEB,**

Además, **ALCAZAR** ofrece el servicio de adaptación de su página web a las exigencias que le impone la **LSSI** (Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico) y sus implicaciones en materia de Protección de Datos de Carácter Personal.

GUÍA PRÁCTICA DE PROTECCIÓN DE DATOS PARA LA EMPRESA

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. ¿EN QUÉ CONSISTE LA PROTECCIÓN DE DATOS?

Es el derecho que tienen todos los ciudadanos a que sus datos personales no sean utilizados sin la autorización y protección debidas de manera que se pueda evitar que, a través de un tratamiento automatizado o manual, se esté en disposición de confeccionar informes o perfiles del titular de los datos que puedan afectar a su intimidad.

Se trata de un derecho fundamental recogido en el artículo 18.4 de la Constitución Española:

"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".

Consiste en síntesis en el ejercicio de control por parte del titular de los datos sobre quien, cómo, para qué, dónde y cuándo son tratados los datos relativos a su persona. Control que se hace efectivo a su vez a través del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

2. CONCEPTOS Y DEFINICIONES

¿ Qué es un dato de carácter personal?
La Ley de Protección de Datos entiende por dato personal cualquier información concerniente a personas físicas identificadas o identificables.

Identificable significa que se pueda por cualquier medio averiguar la identidad de la persona a través de los datos que se manejen.

¿ Qué es un fichero?
Fichero es, a estos efectos, todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

¿ Qué es un tratamiento de datos?
Se entiende por tratamiento de datos las 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.

Es importante matizar que con la vigente Ley Orgánica de Protección de datos ya no solo están incluidos los tratamientos automatizados previstos en la Ley Orgánica de tratamiento Automatizado de Datos, sino también cualquier otro tipo como por ejemplo los tratamientos documentales, de voz o de imagen.

¿ Qué es un responsable del fichero o tratamiento?
Es toda persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

¿ Quién es un afectado o interesado?
Es la persona física titular de los datos que sean objeto del tratamiento de datos.

¿ Qué es un procedimiento de disociación?
Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

¿ Qué es un encargado del tratamiento?
Es la 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.

(La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad que el encargado del tratamiento está obligado a implementar.)

¿Qué es el consentimiento del interesado?
Consentimiento del interesado es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

¿Qué es una cesión o comunicación de datos?
Se entiende por cesión o comunicación de datos toda revelación de datos realizada a persona distinta del interesado.

La cesión de datos se rige por el principio de consentimiento a fin de que sea únicamente el titular de los datos (afectado o interesado) el que tenga el control sobre los mismos.

¿Qué es una fuente accesible al público?
Una fuente accesible al público es aquel fichero 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.

Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.

Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

¿ Qué es un sistema de información?
Es el conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

¿ Qué es un usuario?
Es el sujeto o proceso autorizado para acceder a los datos.

¿ Qué es un recurso?
Es cualquier parte componente de un sistema de información.

¿Qué es la identificación?
Es el procedimiento de reconocimiento de la identidad de un usuario.

¿Qué es la autenticación?
Es el procedimiento de comprobación de la identidad de un usuario.

¿Qué es el control de acceso?
Es el mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

¿Qué es una contraseña?
Es una información confidencial, frecuentemente constituida por una cadena de caracteres que puede ser usada en la autenticación de un usuario.

¿Qué es un bloqueo de datos?
Es la identificación y reserva de datos con el fin de impedir su tratamiento.

3. PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES

La calidad de los datos
El artículo 4 de la Ley Orgánica de Protección de Datos establece que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho 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, todo ello aunque se cuente con la posible autorización del interesado o aunque se cuente con la habilitación legal para someter la información a tratamiento.

No podrán usarse para finalidades incompatibles con aquellas para las que fueron recogidos.
Deberán ser exactos y puestos al día, respondiendo con veracidad a la situacion actual del afectado.
Si no son exactos o están incompletos deben ser cancelados o sustituidos por los correctos.
Serán cancelados cuando dejen de ser necesarios.
No podrán ser conservados (salvo en el caso en que se decida su mantenimiento por valores históricos, científicos o estadísticos) una vez que dejen de ser útiles para la función prevista, con excepción de la legislación específica prevista al efecto (Obligaciones fiscales, Seguros...).
Finalmente se establece la prohibición de recogida de datos por medios fraudulentos, desleales o ilícitos.

Derecho de información en la recogida de datos
Será requisito para la validez del consentimiento que de modo previo e inequívoco se informe al interesado:

- de la existencia de un fichero o tratamiento de datos
- de la finalidad del mismo
- de los destinatarios de la información
- del carácter obligatorio o facultativo de sus respuestas a las preguntas planteadas
- de las consecuencias de la obtención de los datos o de la negativa a suministrarlos
- de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición
- de la identidad y dirección del responsable del fichero.

Cuando se utilicen cuestionarios u otros impresos para la recogida figurarán las advertencias señaladas en los puntos anteriores.

El consentimiento del afectado

Como regla general el tratamiento requerirá consentimiento inequívoco del afectado que se podrá otorgar en cualesquiera de las formas admisibles en Derecho. Podrá otorgarse tácitamente o de modo presunto, salvo para aquellos casos en que la Ley Orgánica prevea que el consentimiento haya de otorgarse expresamente.

Para que no exista vicio del consentimiento y por lo tanto sea válido se requiere que los datos no se recaben por medios fraudulentos, desleales o ilícitos.

El consentimiento podrá ser revocado en cualquier momento por causa justificada, pero no se le podrán atribuir efectos retroactivos a la revocación.

El consentimiento es obligatorio salvo que una ley disponga otra cosa, se trate de datos que se recojan en fuentes accesibles al público, siempre que los datos provengan de ficheros de titularidad privada, que se recojan para el ejercicio de las funciones propias

de las Administraciones Públicas, o que se refieran a personas vinculadas por una relación negocial, laboral administrativa o un contrato o precontrato y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento del mismo, o para proteger su interés vital.

Datos especialmente protegidos

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. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

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.

Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

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, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones necesarias legalmente con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

Por lo que se refiere a los ficheros automatizados de datos les será de aplicación lo previsto en el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

Deber de secreto

La obligación del deber de secreto afecta al responsable del fichero y demás personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal,

incluso después de haber finalizado la relación con el titular o el responsable del fichero.

Comunicación de datos

Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados 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.

Será nulo el consentimiento cuando no conste la finalidad a la que se destinaran los datos o el tipo de actividad de aquel a quien se pretendan comunicar.

No es necesario el consentimiento del afectado para la cesión o comunicación de los datos**:**

a) Cuando la cesión está autorizada en una Ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) 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
d) 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. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f) 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

No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

La ley establece la obligación de que el tratamiento por cuenta de terceros esté regulado en un contrato en el que se hará constar que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los utilizará o aplicará para fines distintos de los previstos en el contrato ni los comunicará a terceras personas. Asimismo en el contrato se establecerán las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

4. NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS

LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPD)

Constituye el núcleo esencial del actual marco normativo en esta materia junto con otras normas generales o sectoriales, de rango legal y reglamentario a las que más adelante nos referiremos.

Con la promulgación de esta Ley se llevó a cabo la transposición de la Directiva 95/46/CEE, del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La Ley Orgánica de Protección de Datos tiene como objeto el garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, especialmente de su honor e intimidad personal y familiar, en lo concerniente al tratamiento de sus datos personales.

Esta Ley supuso la derogación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal que fue la primera ley española de protección de datos y que llenó en su día una laguna en la protección de un derecho reconocido como fundamental.

La LOPD entiende por datos de carácter personal cualquier información sobre las personas físicas identificadas o identificables, tales como:

–Nombre y apellidos, DNI, Dirección, datos bancarios, etc.
–Datos especialmente sensibles: ideología, religión o creencias, raza, salud, vida sexual, afiliación sindical...

REAL DECRETO 1332/1994, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica 5/1992, de 29 e octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal.

Este Real Decreto desarrolla los siguientes aspectos de la derogada LORTAD:

- Plazo en que el responsable del fichero tiene la obligación de hacer efectivo el derecho de rectificación o cancelación del afectado.
- Procedimiento para ejercitar los derechos de acceso, rectificación y cancelación.
- Forma de efectuar las reclamaciones ante el órgano de control por el afectado.
- Extremos que debe contener la notificación de los ficheros para su inscripción en el Registro General de Protección de Datos.
- Procedimiento de inscripción de los ficheros.

- Procedimiento sancionador.

Pese a que como se ha dicho desarrolla a la derogada LORTAD, este Real Decreto se encuentra en vigor en base a lo establecido en la disposición transitoria tercera de la LOPD:

"... continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley".

EL REGLAMENTO DE MEDIDAS DE SEGURIDAD (RD 994/1999, DE 11 DE JUNIO)

El artículo 18.4 de la Constitución Española establece 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".

Como consecuencia de este derecho fundamental y del artículo 9 de la LORTAD (Ley Orgánica 5/92) relativo al necesario desarrollo reglamentario de condiciones de seguridad que garanticen la confidencialidad e integridad de los datos de carácter personal, se aprobó el Real Decreto 994/1999 de 11 de junio sobre medidas de índole técnico y organizativo que deben cumplir las empresas para evitar la posible alteración, pérdida, tratamiento o acceso no autorizado a los ficheros de datos de carácter personal.

Así pues, este reglamento está asociado a la LORTD de 1995 y no a la LOPD, que es posterior, de modo que determina las medidas técnicas y organizativas mínimas que deben establecerse para la información de carácter personal sobre la que se realiza un tratamiento automatizado, no obstante sigue en vigor en base a lo establecido en la disposición transitoria tercera de la LOPD transcrita en el apartado anterior.

El nuevo reglamento establece una serie de medidas de seguridad y sus correspondientes sanciones por incumplimiento de las mismas, destinadas a garantizar la correcta custodia y manipulación de los ficheros afectados y evitar la posible fuga de datos sin su correspondiente consentimiento a empresas o países con menor nivel de protección.

Establece tres niveles de seguridad:
–Básico: cualquier dato de tipo personal, nombre, DNI, dirección, etc.
–Medio: datos de comisión de infracciones penales y administrativas, Hacienda Pública, servicios financieros, ficheros de publicidad.
–Alto: datos sensibles como ideología, religión, raza, salud o vida sexual.

Los plazos máximos que marca la Ley para adaptar los ficheros son:
–26 de diciembre de 1999, prorrogado a 26 de marzo de 2000. Medidas de nivel básico.
–26 de junio de 2000. Medidas de nivel medio.
–26 de junio de 2002. Medidas de nivel alto.

Asimismo, establece la obligación de confeccionar el Documento de Seguridad siempre que se traten datos personales, cualquiera que sea el nivel de seguridad que le correspondan.

El documento de seguridad es una de las partes fundamentales de la protección de datos. Se trata de un documento mediante el cual se elabora y adoptan las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal, su adopción es de obligado cumplimiento para el responsable del fichero, o en su caso, del encargado del tratamiento.

El documento deberá contener, como mínimo, los siguientes aspectos:

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

5. PRINCIPALES OBLIGACIONES DEL RESPONSABLE DEL FICHERO O TRATAMIENTO DERIVADAS DE LA NORMATIVA DE PROTECCIÓN DE DATOS

- Inscripción de los ficheros en el Registro General de la Protección de Datos. Artículo 26 LOPD. Artículos. 5 y 6 R.D 1332/1994, de 20 de Junio.
- Redacción del documento de seguridad. "El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de seguridad de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información" R.D 994/1999, de 11 de Junio.
- Redacción de cláusulas de protección de datos. Artículo 5 LOPD.
- Auditoría. Artículo 17 R.D. 994/1999, de 11 de Junio.
- Implementar las medidas de seguridad de índole técnica y organizativas necesarias para garantizar la seguridad de los datos objeto de tratamiento. Artículos 9 y 10 LOPD y R.D 994/1999, de 11 de junio.
- Redacción de los contratos, formularios y cláusulas necesarias para la recogida de datos, los tratamientos por terceros y las cesiones o comunicaciones de datos.
- Informar al titular de los datos sobre la existencia y finalidad del fichero, quién es el responsable del mismo y de que forma puede ejercer los derechos de acceso, rectificación, oposición y cancelación.
- Obtener el consentimiento del afectado en los casos en que sea preceptivo.
- Respetar la calidad y exactitud de los datos y su utilización exclusivamente para el fin para el que se recogieron.

6. DERECHOS DE LOS AFECTADOS

Dentro de los derechos que corresponden en esta materia a los afectados deben distinguirse dos grupos, por un lado los derechos que constituyen el núcleo esencial del derecho a la protección de datos que son el derecho de acceso, rectificación, cancelación y oposición; y por otro lado el derecho a impugnación, el derecho a indemnización y el derecho a la consulta del Registro General de Protección de Datos.

El derecho de acceso
Es el derecho que tiene todo ciudadano para conocer sus datos personales que figuren en un fichero determinado sometidos a tratamiento, cuál ha sido el origen de éstos, y qué cesiones se han realizado o se prevean realizar en el futuro.

El derecho de acceso se ejerce mediante solicitud dirigida al responsable del fichero y éste deberá responder en el plazo máximo de un mes contestando a los extremos solicitados.

El derecho de rectificación
El titular de los datos podrá solicitar del responsable del fichero la rectificación de los sus datos personales cuando éstos sean inexactos, incompletos, inadecuados o excesivos.

El responsable deberá atender a lo solicitado en el plazo de diez días.

El derecho de cancelación
Cuando el titular de los datos tuviera conocimiento de que sus datos personales tratados en un fichero son inexactos o incompletos, inadecuados o excesivos, podrá solicitar del responsable del fichero la cancelación de los mismos.

El responsable deberá atender la petición en el plazo de diez días.

El derecho de oposición
En aquellos casos en los que no resulta necesario el consentimiento del interesado para el tratamiento de sus datos, éste podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos, siempre que una Ley no disponga lo contrario.

El responsable del fichero procederá a la exclusión de los datos relativos al afectado.

Derecho de impugnación
El afectado podrá impugnar aquellas decisiones que tengan efectos jurídicos y cuya base sea únicamente un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Derecho a indemnización
En aquellos casos en que a consecuencia del incumplimiento de lo dispuesto en la Ley Orgánica 15/1999 el afectado sufra daño o lesión en sus bienes o derechos, éste tendrá derecho a una indemnización.

Derecho de consulta al Registro General de Protección de Datos
Se trata del derecho de los interesados o afectados a recabar información del Registro General de Protección de Datos sobre la existencia de ficheros que traten datos personales, la finalidad de éstos y la identidad del responsable del fichero.

7. LA AGENCIA DE PROTECCIÓN DE DATOS

La Agencia de Protección de Datos es un Ente de Derecho Público, creado con la finalidad de velar por el cumplimiento de la normativa sobre protección de datos personales informatizados y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, oposición, rectificación y cancelación de datos.

La Agencia desarrolla así una labor imprescindible en pro de la garantía del derecho fundamental a la protección de datos personales, no siempre justamente valorada y tampoco suficientemente conocida, apareciendo frecuentemente no tanto como autoridad de garantía del derecho sino como entidad sancionadora.

Administra el Registro General de Protección de Datos, que es el órgano al que corresponde velar por la publicidad de la existencia de los ficheros de datos de carácter personal.

Realiza inspecciones en las empresas a instancia de los afectados o de oficio.

Dicta instrucciones y recomendaciones que sean precisas para adecuar los tratamientos a los principios de la LOPD.[1]

Es competente para instruir y resolver los expedientes sancionadores por la comisión de las infracciones previstas en la ley:

INFRACCIONES LEVES.-

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

---

[1] Las instrucciones dictadas hasta la fecha por la Agencia de Protección de Datos son las siguientes:

- INSTRUCCIÓN 1/95*, de 1 de marzo de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito*.
- INSTRUCCIÓN 2/1995*, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.*
- INSTRUCCIÓN 1/1996*, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios*
- INSTRUCCIÓN 2/1996*, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo*
- INSTRUCCIÓN 1/98*, de 19 de Enero, de La Agencia de Protección de Datos, relativa al Ejercicio de los Derechos de Acceso, Rectificación y Cancelación.*
- INSTRUCCION 1/2000*, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.*

b) 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.

c) 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.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave

La prescripción de la infracción Leve: 1 año

INFRACCIONES GRAVES.-

a)Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.

b) 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 constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter

personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

La prescripción de la infracción Grave: 2 años.

INFRACCIONES MUY GRAVES.-

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una Ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) 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.

f) 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 g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

La prescripción de la infracción Muy Grave: 3 años.

SANCIONES.-

Leves: 601,01 € a 60.101,21 €

Graves: 60.101,21 € a 300.506,05 €

Muy graves: 300.506,05 € a 601.012,10 €

La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

8. ESPECIAL REFERENCIA A LOS CÓDIGOS TIPO

Los códigos tipo están regulados en el artículo 32 del la LOPD y se pueden definir como códigos deontológico o de buena conducta o práctica profesionales. Dichos códigos hacen alusión a la política concreta de la empresa en cuanto a cómo llevará a cabo lo establecido por la ley.

Su elaboración es voluntaria, puesto que para cumplir con los preceptos de la ley sólo hace falta respetar lo en ella establecido.

Pues tendría dos : por un lado, cara al ciudadano, o al consumidor o potencial cliente, se le estará dando la imagen de que el suscriptor del código tipo pone un interés o esmero especiales a la hora de respetar los derechos de los mismos contemplados en la ley; por otro, ante la propia Administración, esto es, ante la Agencia de Protección de Datos, pues dado que los códigos han de inscribirse en el Registro General de Protección de Datos, previo examen de los mismos, estaremos ante un conjunto de normas que, si pasan dicho examen, tendrán el visto bueno de la Agencia de Protección de Datos, de manera que si en algún momento ésta intenta sancionar a la empresa por alguna práctica de protección de datos, que considere ilegal, y dicha práctica no se ha separado

de lo establecido en el código tipo, estaría contradiciéndose, contradicción que iría a favor de quien suscribió el código tipo.

ANEXO I

LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPD)

ANEXO II

REAL DECRETO 1332/1994, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica 5/1992, de 29 e octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal

ANEXO III

REAL DECRETO 1332/1994, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica 5/1992, de 29 e octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal.