DOSSIER INFORMATIVO

PROTECCIÓN DE DATOS

PRESENTADO POR

ICEF
Consultores

ICEF Consultores
Calle Velázquez, 94 – 1ª Planta
28006 Madrid
Telf. 91.781.34.07
Fax: 91.781.20.70
www.icefconsultores.com

INDICE

ADAPTACIÓN DE LAS EMPRESAS EN MATERIA DE PROTECCIÓN DE DATOS

ADAPTACIÓN DE LAS EMPRESAS A LA SOCIEDAD DE LA INFORMACIÓN

ANEXO

ADAPTACIÓN DE LAS EMPRESAS EN MATERIA DE PROTECCIÓN DE DATOS

1. INTRODUCCIÓN

La protección de datos en las empresas es necesaria, ya no sólo desde una óptica externa o legal, como cumplimiento a la normativa vigente en materia de protección de datos (**Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal** -en adelante, **LOPD**-; y el actual **RD 1720/2007 de Desarrollo de la Ley Orgánica de Protección de Datos 15/99**, que ha derogado desde abril de 2008 el antiguo **Reglamento de Medidas de Seguridad aprobado 994/1999** que regulaba la materia, lo que ha introducido diversos cambios en la normativa aplicable y, especialmente en materia de ficheros soporte papel. Así mismo, es de especial importancia la adaptación de las empresas a dicha normativa, ya sólo por su imperativo legal, sino en orden a mantener una organización interna efectiva de la empresa que evite vulneraciones en el tratamiento de datos personales, así como en aras a evitar posibles sanciones que oscilan entre los **900 €** y los **600.000 €.**

La obligación del cumplimiento de la normativa sobre protección de datos de carácter personal está especialmente ligada con la actividad diaria de las empresas, puesto que éstos son un activo importante para el quehacer de las mismas. El tratamiento de datos personales está ocasionando importantes riesgos económicos asociados al incumplimiento de la normativa vigente en materia de protección de datos personales. El desarrollo de la actividad de la mayoría de las empresas obliga al establecimiento y adopción de una serie de medidas legales, técnicas y organizativas de seguridad que limiten su responsabilidad frente a posibles incumplimientos de la normativa. **ICEF** Consultores considera que esta adaptación ha de realizarse de una forma exhaustiva y personal acorde a los diferentes ámbitos de actuación y desarrollo empresarial, puesto que entendemos que cada empresa es diferente, inclusive dentro del mismo sector de actividad.

Esta situación hace que **ICEF** Consultores exponga el presente dossier informativo con el fin de presentarles de una forma, sencilla y clara, las obligaciones y deberes que exige la normativa en materia de protección de datos y las medidas a adoptar para adecuar su organización o empresa.

2. PANORAMA LEGAL

La protección de datos personales se encuentra regulada en la **LOPD** y en el **RD 1720/2007** -en adelante, **RDLOPD**- normativa que es de obligado cumplimiento para las empresas y autónomos, indistintamente de su tamaño, organización o ámbito de actividad. El objetivo de la mencionada normativa es la **protección que de los datos personales realiza la empresa**, entendiéndose por dato personal *cualquier información concerniente a personas físicas identificadas o identificables*, es decir, aplicable a la información que la empresa pueda disponer de sus trabajadores, proveedores, clientes, etc. Además, dicha normativa regula el **tratamiento** de esos datos, es decir, *todas aquellas 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*.

El período de adaptación para los datos que son tratados en ficheros automatizados y soporte papel ha finalizado ya. Esta situación supone que a fecha de hoy, todas las empresas que traten datos de carácter personal han de estar completamente adecuadas a la normativa.

La adaptación a la normativa de protección de datos, ya no es sólo un requisito legal y económico, sino que además es imprescindible, de cara a mejorar la imagen de la empresa, en relación a clientes, proveedores, etc.

Otro punto importante es el que hace referencia al Organismo encargado de velar por el cumplimiento de la normativa referida, la Agencia Española de Protección de Datos (en adelante, **AEPD**). Dicho organismo impone importantes sanciones a todas aquellas personas físicas o jurídicas que infrinjan la normativa aplicable, pudiendo llegar a alcanzar dichas sanciones la cifra de **600.000 € (100 millones de pesetas)**. Concretamente, la **AEPD** ha recaudado el pasado año la cantidad de **20 millones de euros** en concepto de sanciones.

3. OBLIGACIONES Y DEBERES RESPECTO A LA LOPD

La **LOPD** es de aplicación a *todos los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado*. Lo cual significa que todos los datos personales, entendiendo por éstos -*cualquier información concerniente a personas físicas identificadas o identificables*-, deben adecuarse a la citada ley con el objeto de que se garanticen y protejan las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Las obligaciones y deberes que establece la **LOPD** para garantizar la confidencialidad de los datos de carácter personal son:

1. Inscripción de ficheros

Todos los datos personales necesarios para el logro de la actividad -bases de datos de clientes, pacientes, proveedores, facturación, currículos, nóminas, etc.- tienen que ser notificados e inscritos en la **AEPD**, debiéndose mantener actualizada la finalidad de cada uno de los ficheros.

2. Medidas de seguridad

Todos los ficheros deberán adoptar medidas de índole técnica y organizativa para garantizar la seguridad de los datos de carácter personal que contienen, evitando así la alteración, pérdida, tratamiento o acceso no autorizado. Las medidas de seguridad exigibles por el **RD 1720/2007** se clasifican en tres niveles: básico, medio y alto.

- **Básico**; se considerarán ficheros de nivel básico, aquellos que contengan nombres, apellidos, edad, lugar de nacimiento, profesión, teléfono, etc.

- **Medio**; aquellos ficheros que contengan datos relativos a la comisión de infracciones administrativas, penales, Hacienda Pública, servicios financieros y los de solvencia patrimonial. También se considerarán ficheros de nivel medio, aquellos que contengan un conjunto de datos de carácter

personal suficientes que permitan obtener la evaluación de la personalidad de un individuo, así como otros perfiles más específicos introducidos por el Nuevo Reglamento.

- **Alto**; serán todos aquellos ficheros que contengan datos de 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 y datos de violencia de género, entre otros. Así como otros perfiles más específicos introducidos por el Nuevo Reglamento.

3. Documento de seguridad

Conjunto de medidas a implantar donde se especifica la normativa interna de obligado cumplimiento para el personal con acceso a los datos y a los sistemas de información de seguridad.

4. Auditoria

Procedimiento mediante el cual se verificará el cumplimiento de la normativa en materia de protección de datos -**LOPD**, **RDLOPD**, **Instrucciones AEPD**, **etc**.-. Dicho procedimiento deberá realizarse, al menos, cada dos años para los ficheros con un nivel de seguridad medio u alto. Este informe permitirá establecer el grado de adecuación de la empresa, entidad u organización a las medidas técnicas, organizativas y legales.

4. PRINCIPIOS E INFRACCIONES

El correcto tratamiento de los datos de carácter personal, por parte de las empresas, instituciones u organizaciones, descansa en los principios recogidos en la **LOPD**, los cuales son de obligado cumplimiento y cuya omisión es tipificada como infracción -**leve, grave y muy grave**-, sancionándose con importes que alcanzan o superan los **600.000 €** (**100 millones de pesetas**).

A continuación se detallan los principios, infracciones y sanciones que son establecidos por la **LOPD**.

1. Calidad de los datos

El **artículo 4 LOPD** hace referencia a este principio. En este sentido, la recogida y el tratamiento de los datos ha de realizarse cumpliendo los criterios de calidad exigidos, es decir, deberán adecuarse a la finalidad para la cual fueron recabados, ser pertinentes y no excesivos en relación con la finalidad que justifica su recogida; han de ser recogidos de forma lícita, deben ser exactos y puestos al día; y no podrán mantenerse indefinidamente sin justificación. Por lo tanto, el principio de calidad recae en cuatro requisitos de obligado cumplimiento:

- **Finalidad:** Los datos sólo podrán ser recogidos para su posterior tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explicitas y legítimas para las que se hayan obtenido.

- **Utilización no abusiva, ni excesiva:** Los datos no podrán ser utilizados para finalidades incompatibles con aquellas que hubiesen justificado su recogida. Sin embargo, como importante excepción, la **LOPD** no considera incompatible el tratamiento posterior de los datos con fines históricos, científicos o estadísticos.

- **Exactitud:** Los datos deberán ser exactos y puestos al día de forma que respondan con veracidad a la situación actual de su titular.

- **Legalidad en la recogida:** La ley impone una obligación de lealtad al responsable del fichero, prohibiendo la recogida de datos por medios ilícitos, desleales o fraudulentos.

El incumplimiento de este principio, es un hecho constitutivo de **infracción grave**, cuya multa oscila de **60.101,21 € a 300.506 €**.

2. Cumplimiento del deber de información

La LOPD, en su artículo 5, obliga a que con carácter previo a la recogida de los datos personales, se informe a su titular de los siguientes extremos:

- 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.

- Del carácter obligatorio o facultativo de las respuestas a las preguntas que le sean formuladas, así como de las consecuencias de no facilitar los mismos.

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

- De la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.

- De la identidad y dirección del responsable del tratamiento o, en su caso, su representante.

El incumplimiento de este deber de información es un hecho constitutivo de infracción, cuya sanción es la imposición de una multa que oscila de **900 € a 40.000 €**.

3. Consentimiento del afectado

El tratamiento de los datos de carácter personal requerirá como regla general, salvo en los casos en los que la ley expresamente disponga lo contrario, el consentimiento

inequívoco del afectado **(artículo 6 LOPD)**, pudiendo ser dicho consentimiento tanto expreso como tácito. Además, el consentimiento dado por el interesado al responsable del tratamiento podrá ser revocado cuando exista causa justificada, si bien dicha revocación nunca tendrá atribuidos efectos retroactivos.

El incumplimiento de esta obligación implica un hecho constitutivo de **infracción grave**, que se encuentra tipificado en la **LOPD,** cuya sanción es la imposición de una multa que oscila de **40.000 € a 300.000 €**.

4. Régimen de comunicaciones o cesiones de datos

El término *"comunicación de datos"* hace referencia a cualquier revelación de datos personales realizada a una persona distinta del interesado. La **LOPD** incorpora un concepto de cesión y comunicación excesivamente extenso. Para una mejor comprensión de esta obligación acotaremos el campo de actuación a los siguientes extremos:

- La comunicación o cesión de los datos es un de tipo de tratamiento de datos personales, de forma que deben tenerse en cuenta, el deber de información y solicitud del consentimiento del interesado para el tratamiento de los datos personales.

- La principal consecuencia de la cesión de datos a un tercero es que este, al que se le ceden los datos, pasará a tener la consideración de un nuevo responsable del tratamiento.

- Como regla general y de acuerdo con el **artículo 11 apartado primero de la LOPD**, los datos de carácter personal objeto del tratamiento sólo podrán ser cedidos o comunicados para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado.

- El responsable del fichero, en el momento de efectuar la primera cesión de datos, **artículo 27 LOPD**, deberá informar, a los titulares de los datos de

carácter personal, de la primera cesión efectuada, así como de la finalidad del fichero al que han sido cedidos, la naturaleza de los datos cedidos y el nombre y dirección del cesionario. Se trata pues, de una específica obligación de información, ya que sólo debe cumplirse cuando se realice la primera cesión de datos. Dicha obligación está exceptuada para los casos que, expresamente, recoge el **artículo 11 apartado segundo de la LOPD**.

El incumplimiento de esta obligación, es un hecho constitutivo de **infracción muy grave**, cuya multa oscila de **300.000 € a 600.000 €**.

5. Régimen de encargados del tratamiento

La relación de encargado del tratamiento se encuentra regulada en el **artículo 12 LOPD**. Según se desprende del mismo, no se considerará comunicación o cesión de datos personales el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. Es decir, o estamos ante una cesión de datos, o estamos ante un encargo de tratamiento de los datos.

El responsable del fichero es el que facilita al encargado del tratamiento los datos personales que éste último debe tratar (recoger, grabar, actualizar, conservar, modificar, bloquear o cancelar, entre otros) por cuenta del primero. Por tanto, la prestación de servicios por cuenta de terceros diferentes al responsable del fichero, desde el momento en que exigen el tratamiento de datos personales y, por tanto, el acceso a los mismos, se constituye una relación de encargado de tratamiento que la **LOPD** obliga a regular por medio de un contrato, debiendo figurar por escrito o de cualquier otra forma que permita acreditar su celebración y contenido.

El incumplimiento de esta obligación, presente en la normativa de protección de datos, es un hecho constitutivo de **infracción grave**, cuya multa oscila de **40.000 € a 300.000 €**.

6. Cumplimiento del deber de secreto

El deber de guardar secreto, recogido en el **artículo 10 LOPD**, respecto de los datos personales a los que se tenga o se haya tenido acceso como consecuencia de las

funciones efectivamente desarrolladas es uno de los principales y más importantes deberes y obligaciones que recaen, no sólo respecto del responsable del fichero, sino respecto de todos aquellos que intervengan en cualquier fase del tratamiento de los datos personales. Dicho deber tiene un carácter extensivo, es decir, permanece en el tiempo, a pesar que el tratamiento de los datos personales haya terminado.

La infracción de este deber de secreto puede ser constitutiva, en función del tipo de datos respecto de los cuales se infrinja el deber, de **infracción leve** -cuando la infracción no es calificable como grave o muy grave-, **infracción grave** -si el fichero contiene datos relativos a la comisión de infracciones penales o administrativas, datos de Hacienda Pública, servicios financieros, datos de solvencia patrimonial o si

el fichero contiene un conjunto de datos personales suficientes para obtener una evaluación de la personalidad del individuo- o, **infracción muy grave** -cuando el fichero contiene datos de los calificados como especialmente protegidos-. Así se recoge en el articulado de la **LOPD**, más concretamente en su **artículo 44**, y cuyo incumplimiento está sancionado con multas que oscilan desde los **900 € a 600.000 €**.

7. Ejercicio efectivo de los derechos ARCO

Los **artículos 15, 16 y 17 de la LOPD** recogen estos derechos de los afectados otorgando a los mismos una serie de facultades sobre sus datos personales cuando estos se encuentran en un fichero automatizado y estén siendo objeto de tratamiento. Atendiendo a los artículos anteriormente citados, entre los extremos a tener en cuenta para el adecuado cumplimiento se encuentran los siguientes:

- Informar a los afectados cuando se recogen sus datos personales de la posibilidad de ejercitar los derechos de acceso, oposición y cancelación.

- El lugar y forma de ejercitarlos.

- Mecanismos para atender las distintas solicitudes de ejercicio de estos derechos por parte de los afectados.

- Medios tecnológicos para eliminar los datos, una vez cancelados. La cancelación de los datos implica, con carácter general, su borrado físico, si bien en determinadas ocasiones (cuando razones técnicas lo imposibiliten) bastaría con su bloqueo, que evitase la posterior utilización o acceso a los datos.

El incumplimiento de estos deberes y obligaciones, es un hecho constitutivo de **infracción leve, grave o muy grave, atendiendo a las circunstancias de cada caso puntual**, cuya multa oscila de **900 € a 600.000 €**.

5. PLAN DE ADAPTACIÓN

La adecuación en materia de protección de datos de carácter personal que proponemos -siempre orientativa bajo nuestra experiencia- abarcaría las siguientes fases de actuación:

PLAN DE ADAPTACIÓN	
Fase 1ª	Estudio, verificación e identificación de los datos de carácter personal
Fase 2ª	Estudio del contenido de información: Nivel y Medidas de Seguridad
Fase 3ª	Deficiencias detectadas y Recomendaciones realizadas
Fase 4ª	Ejecución de la adecuación
Fase 5ª	Inscripción y modificación de ficheros ante la AEPD

6. FASES DE LA ADAPTACIÓN

6.1. Estudio, Verificación e Identificación de los datos de carácter personal

En la primera fase del Proyecto de Adaptación se procedería al estudio, verificación e identificación de todos y cada uno de los elementos necesarios para llevar a cabo la completa adaptación, procediéndose a examinar los datos de carácter personal objeto de tratamiento.

En dicha fase de actuación se procedería a examinar entre otros aspectos:

- **Obtención de los datos de carácter personal.** En este apartado se examinarían las distintas formas de recogida de datos (cartas, teléfono, tarjetas, formularios, propio afectado o interesado, Página Web, etc.)

- **Finalidad de los datos de carácter personal.** Examen del fin de la recogida, es decir, para qué se van a tratar los diferentes datos recogidos.

- **Ficheros de datos de carácter personal.** Estudio de los diferentes ficheros que contienen datos de carácter personal. Se verificaría la cantidad de ficheros existentes, dándose recomendaciones en cuanto a ficheros obsoletos o repetidos, el soporte (informático, papel, etc.) en el que se encuentran, ubicación de los mismos, etc.

- **Consentimiento del afectado en la recogida de los datos.** Procedimiento que tiene como finalidad identificar si el proceso de recogida de datos alcanza el suficiente grado de conocimiento a la finalidad comunicada al afectado o interesado.

- **Responsable del fichero.** Identificar quién es la persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento.

- **Derecho de los afectados.** Estudio y verificación de los procesos para dar cumplimiento al derecho que ostentan los afectados en materia de acceso, rectificación, cancelación, oposición al tratamiento de los datos, consulta al Registro General de Protección de Datos, etc.

- **Encargo de Tratamiento.** Examen de los diferentes servicios que pueden ser prestados por terceros en nombre de **la empresa o responsable del fichero** o viceversa, como por ejemplo la posibilidad de que una gestoría pudiera llevar el tratamiento de las nóminas de los trabajadores a efectos fiscales. Se identificarían todos y cada uno de los supuestos en los que el **responsable del fichero** sea encargado de tratamiento y no responsable del mismo, como aquellos supuestos en los que terceras empresas traten datos en nombre de aquel.

- **Acceso a los datos de carácter personal.** Evaluación de la organización para identificar el proceso de acceso a los datos de carácter personal, identificando las medidas técnicas adoptadas (usuario, password, copias de seguridad, gestión de soportes, etc.)

- **Cesión de datos.** Es el punto más controvertido en el Proyecto de Adecuación, puesto que la **LOPD** prohíbe, expresamente, la cesión de datos a excepción de ciertos supuestos tasados. Es por ello, que en este ámbito se haría un estudio pormenorizado de los siguientes puntos: cesión de datos a terceros; necesidad o no de consentimiento; cesión de bases de datos; revisión de contratos que tienen como finalidad el tratamiento de datos de carácter personal; pertenencia de la empresa como filial o supuestos de casos de fusión o escisión, puesto que estaríamos ante personalidades jurídicas diferentes.

6.2. Niveles de Seguridad

Una vez estudiados los datos obtenidos en la primera fase del Proyecto de Adecuación en materia de protección de datos, se procedería a identificar el nivel de seguridad en base a la naturaleza de la información que contengan los diferentes datos que son tratados, por parte de la **empresa** o **responsable del fichero**. En concreto, los diferentes ficheros que contengan datos personales serían organizados en función del nivel de seguridad:

- **Básico**; se considerarán ficheros de nivel básico, aquellos que tengan nombres, apellidos, edad, lugar de nacimiento, profesión, teléfono, etc.

- **Medio**; aquellos que contengan datos relativos a la comisión de infracciones administrativas, penales, Hacienda Pública, servicios financieros y los de solvencia patrimonial. También se considerarán ficheros de nivel medio, aquellos que contengan un conjunto de datos de carácter personal suficientes que permitan obtener la evaluación de la personalidad de un individuo.

- **Alto**; serán todos aquellos ficheros que contengan datos de 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.

Así mismo, en función del nivel de seguridad, se reflejarían las medidas a adoptar para cada uno de los ficheros y, en consecuencia, definiendo y estableciendo las medidas técnicas, organizativas y legales para su adecuación al **RDLOPD**.

6.3. Deficiencias y Recomendaciones

Bajo esta fase se hace alusión al "**Documento Legal"**, en el que se reflejarían, tras el estudio y revisión de todos los elementos en los que se basa dicho Proyecto de Adecuación, las deficiencias detectadas y las recomendaciones que, a tal efecto, se plasmarían para una mejor adaptación de la **empresa** a la normativa vigente en materia de protección de datos de carácter personal.

En el Documento Legal se haría referencia a los siguientes parámetros:

- **Introducción**, en la que se reflejaría el por qué de la necesidad de la empresa a adecuarse a la normativa de protección de datos, los recursos utilizados para la realización del proyecto, los ficheros existentes con anterioridad al inicio del Proyecto de Adecuación, etc.

- **Panorama legal** en materia de protección de datos, haciendo hincapié en supuestos de dudosa aplicación, las medidas para los ficheros en soporte papel, algunas recomendaciones de la **AEPD**, los diferentes aspectos relevantes de la normativa en materia de protección de datos de carácter personal, etc.

- **Las deficiencias detectadas y las recomendaciones** que se realizan a las mismas, tanto en el ámbito legal, como en el ámbito de aplicación de las medidas de seguridad. Para ello, se examinará el grado de adecuación de la **empresa** a las obligaciones, deberes y exigencias aplicables según la **LOPD** y **DLOPD**.

- **Redacción de los diferentes anexos** que complementarían al Documento Legal y que son imprescindibles para subsanar las deficiencias detectadas.

6.4. Ejecución del Proyecto de Adecuación

Tras la conclusión de las tres primeras fases del Plan de Adecuación a la normativa de protección de datos de carácter personal, se procedería a ejecutar las acciones que a continuación se detallan:

- **Documento de Seguridad**, en el que se describen las normas que, en materia de protección de datos, deberá seguir o aplicar la entidad.

- **Incorporación de las cláusulas** de protección de datos en los diferentes contratos.

- **Elaboración de contratos** de acceso a datos por cuenta de terceros.

- Elaboración del documento **"Obligaciones y Funciones del Personal"**. Normativa interna en la que se detallan los diferentes aspectos a tener en cuenta en materia de protección de datos, por parte del equipo humano que conforma la **empresa**.

- **Asesoramiento técnico y jurídico** para la correcta implantación del Proyecto de Adecuación en materia de protección de datos.

- Redacción del documento **"Inventario de Ficheros"**, en el que se indican los ficheros, la ubicación, el departamento y el nivel de seguridad con anterioridad al Proyecto de Adecuación y, los ficheros que se inscribirían y modificarían ante la **AEPD**.

6.5. Inscripción y modificación de ficheros ante la AEPD

Una vez ejecutada la adecuación en materia de protección de datos, se procedería a la inscripción y modificación del inventario de los ficheros ante la **AEPD**. El proceso de inscripción se realizará *in situ* o telemáticamente.

Se debería completar el formulario de inscripción que a tal efecto dispone la **AEPD** para que, una vez completado, sea presentado y sellado, en la Oficina Central de la **AEPD**, el original y copia.

ADAPTACIÓN DE LAS EMPRESAS A LA SOCIEDAD DE LA INFORMACIÓN

1. APROXIMACIÓN GENERAL

Todos los servicios de la sociedad de la información que sean prestados a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario, o bien que no siendo remunerados por sus destinatarios constituyan una actividad económica para el prestador de servicios, han de cumplir con la normativa de servicios de la sociedad de la información -**LSSI**-.

Con motivo de la entrada en vigor de la **Ley 32/2003**, de 3 de noviembre, **General de Telecomunicaciones**, se han reformado ciertos aspectos de la **Ley 34/2002**, de 11 de julio, **de Servicios de la Sociedad de la Información y Comercio Electrónico**, especialmente, en el ámbito de la protección de los datos personales en las comunicaciones electrónicas.

2. ASPECTOS RELEVANTES

Las empresas, instituciones, fundaciones, etc., por estar encuadradas dentro del ámbito de aplicación de la normativa de servicios de la sociedad de la información, han de cumplir con determinadas obligaciones y deberes, que se resumen en líneas generales de la siguiente forma:

1. Información legal

El **artículo 10 LSSI** exige a los prestadores de servicios la incorporación de cierta información, la cual ha de aparecer en su Web Site de una forma clara, sencilla y gratuita. Entre la información general a incorporar hay que destacar:

- Nombre o denominación social.
- Domicilio social.
- Autorización administrativa si la hubiere.
- Códigos de conducta a los que estuviere adherido, etc.

Junto a la información general obligatoria hay que anexar la información legal específica de la actividad a desarrollar, siempre que ésta esté regulada. En este caso hay que añadir a la información general, expuesta con anterioridad, la siguiente a destacar:

- Datos del Colegio Profesional.
- Normas profesionales aplicables al colectivo, etc.

2. Deber de colaboración y responsabilidades

Todos los prestadores de servicios de la sociedad de la información han de colaborar con los órganos competentes y supervisores en la materia, además de contar con un sistema organizado de almacenamiento de datos, transmisión o modificación de los mismos.

3. Comunicaciones electrónicas

Como hemos apuntado anteriormente, la entrada en vigor de la **LGT** ha supuesto un cambio en el campo de las comunicaciones electrónicas destinadas a los usuarios de los servicios que prestan las diferentes empresas, instituciones o fundaciones. En este sentido, los prestadores de servicios se encuentran expuestos a las sanciones de la **AEPD** por utilizar los datos de los usuarios o clientes, bien para el envío de comunicaciones electrónicas no solicitadas, bien por la omisión del consentimiento, bien por eludir la incorporación de mecanismos que permitan revocar ese consentimiento inicial.

En este sentido, las sanciones se equiparan a las impuestas por la **AEPD** en materia de protección de datos, es decir, sanciones que oscilan entre los **30.000 €** a **600.000 €**. Esto supone una novedad respecto a años anteriores, puesto que se le ha otorgado a la **AEPD** la función de órgano supervisor y sancionador en materia de servicios de la sociedad de la información, más concretamente, en materia de tratamiento de datos personales en las comunicaciones electrónicas.

4. Contratación electrónica

Las exigencias establecidas para aquellos prestadores de servicios que entre sus actividades se encuentre el comercio electrónico -p.e. hacerse socio a cambio de un precio, compra de un determinado material, descarga de música, etc.-, son aún mayores, puesto que han de cumplir con una serie de requisitos de información durante todo el proceso que dura la compra del servicio o producto.

5. Cookies

Con la entrada en vigor del **Real Decreto Ley 13/20012** que transpone las **Directivas 2009/136/CE** y **2009/140/CE** se recoge y modifica la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico en cuanto a la protección de los consumidores y/o usuario de Internet respecto al consentimiento, por parte de aquellos, de programas que recaben datos de navegación -cookies- debiendo, en todo caso, de informar a éstos de los procedimientos para poder impedir dicha recogida de datos.

3. CONSECUENCIAS

Todas aquellas empresas que presten servicios de la sociedad de la información y que no se encuentren totalmente adaptadas a la **LSSI** y a la normativa que le es de aplicación se exponen, ya no sólo a ser sancionadas con multas que pueden llegar a ser desorbitadas, sino que además su prestigio como marca se ve deteriorado de cara a terceros -clientes, usuarios, proveedores, etc.-

Junto a lo expuesto con anterioridad hemos de señalar que la adaptación de los prestadores de servicios a la normativa expuesta, hace que todos los usuarios y destinatarios de su Web Site vean su empresa, institución u organización como aquella con la que poder realizar gestiones de una forma segura y fiable.

ANEXO I. TABLA DE OBLIGACIONES Y SANCIONES

Obligaciones	Resultado por Incumplimiento
Informar al afectado de la recogida de datos de carácter personal. Inscripción de fichero ante la Agencia Española de Protección de Datos. Hacer efectivo el derecho de rectificación o cancelación del interesado en un plazo de 10 días. Secreto profesional y deber de guardar los datos. Proporcionar la información que solicite la Agencia Española de Protección de Datos.	**Infracción LEVE** **(multa de 900 a 40.000 €)**
Recabar el consentimiento expreso del afectado cuando la ley así lo especifique. Poner a disposición del afectado sus derechos de acceso y oposición, así como la posibilidad de no facilitar información. Principio de calidad de los datos, estos tendrán que ser adecuados, pertinentes y no excesivos, en otro caso deberán ser cancelados. Deber de secreto respecto de los datos personales suficientes para obtener una evaluación de la personalidad del individuo. Inscripción del fichero cuando el Director de la AEPD así lo requiera. Cumplir con las medidas de seguridad que por vía reglamentaria se determinen. Deber de información al afectado.	**Infracción GRAVE** **(multa de 40.001 a 300.000 €)**
Comunicación o cesión de datos sólo para el cumplimiento de fines relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. Deber de secreto respecto de los datos especialmente protegidos. Mantener unas medidas de seguridad equiparables a las españolas a la hora de transferir datos a otros países.	**Infracción MUY GRAVE** **(multa de 300.001 a 600.000 €)**