EHLABE
Inclusión sociolaboral de personas con discapacidad
Euskal Herriko Lan Babestuaren Elkartea

MANUAL DE PROTECCION DE DATOS DE CARACTER PERSONAL

EHLABE

Junio 2016

INDICE

1 PRESENTACION

La finalidad de este manual es describir "**los conceptos básicos**" en materia de Protección de Datos de Carácter Personal al objeto de darlos a conocer entre las personas empleadas de:

- ✓ **EHLABE.**

El derecho a la "**Protección de Datos de Carácter Personal**" consiste en el poder que tiene todo individuo de disponer y controlar sus datos personales, lo cual le faculta para decidir cuáles de estos datos facilita a un tercero, o cuáles puede ese tercero recabar. Asimismo, permite al individuo saber quien posee sus datos personales y con qué finalidad, pudiendo oponerse a la posible utilización de sus datos por terceros no autorizados.

La Ley Orgánica 15/1999 de 13 de diciembre Protección de Datos de Carácter Personal, tiene por objeto garantizar y proteger, el tratamiento a los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.

Por todo ello, cualquier empresa o entidad que maneje datos de carácter personal con diferentes finalidades (gestión de personal, proveedores, y clientes) está obligada a garantizar el derecho fundamental a la protección de los datos personales de los que dispone.

2 MARCO LEGAL

- **LOPD:** Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Esta ley garantiza y protege todo lo relativo a los datos personales y establece una serie de obligaciones relativas a la recogida de los datos, consentimiento, conservación, uso, datos especialmente protegidos, etc.

- **RDLOPD:** Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados y en formato papel, que contengan datos de carácter personal. En el Reglamento se establecen las medidas que se han de adoptar obligatoriamente para garantizar la seguridad respecto de los ficheros automatizados, los centros de tratamiento, locales, equipos, etc.

- **LSSI**: Ley 34/2002, de 11 de julio de servicios de la sociedad/empresa de la información y de comercio electrónico.

- **LGT**: Ley 32/2003, de 3 de noviembre General de Telecomunicaciones.

- **Ley 29/2009**, de 30 de Diciembre, por la que se modifica el régimen legal de la competencia desleal y de la publicidad para la mejora de la protección de los consumidores (Listas de Exclusión Robinson).

- **Ley 25/2009 del 27 de Diciembre** (conocida como Ley Ómnibus), donde se refleja la modificación sobre la instalación de los sistemas de Videovigilancia y Ley 23/1992 de 30 de Julio de Seguridad Privada, reguladora de las instalaciones de seguridad con motivo de la seguridad en zonas públicas y privadas.

- **Ley 2/2011, de 4 de marzo**, de Economía Sostenible, disposición final quincuagésima modificaciones en el Titulo VII de la Ley Orgánica 15/1999, LOPD, en referencia a la modificación del régimen sancionador.

- **Real Decreto Ley, de 30 de Marzo de 2012**, en virtud de cual se modifica la LSSI, en relación al uso de las cookies y la publicidad comercial no deseada (SPAM) a través de correo electrónico.

- **INSTRUCCIONES DE LA AGENCIA ESPAÑOLA DE PROTECCION DE DATOS:**

    - **Informe 0086/2010**, de la AEPD, relativo a la cesión de datos de carácter personal de los clientes a la Policía.

    - **Instrucción 1/2006**, de 12 de diciembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

    - **Instrucción 1/2004**, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones.

    - **Instrucción 2/1996**, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.

- **Instrucción 1/1996**, de 1 de marzo, de la APD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.

- **Instrucción 2/1995**, de 4 de mayo, de la APD, sobre garantía de los datos personales recabados en la contratación de seguro de vida de forma conjunta con un préstamo hipotecario o personal.

- **Instrucción 1/1995** de la AEPD relativa a la prestación de servicio sobre solvencia patrimonial y crédito.

3 INTRODUCCION A LA PROTECCION DE DATOS: INTIMIDAD, PRIVACIDAD Y PROTECCION DE DATOS DE CARACTER PERSONAL

3.1 ¿QUE ES LA INTIMIDAD?

Según el diccionario de la RAE, por intimidad se debe entender una *"zona espiritual íntima reservada de una persona o de un grupo, especialmente de una familia".*

El derecho a la intimidad protege la parte más íntima de una persona, esto es, esa esfera personal que define qué es y qué no es privado. Dicho de otra forma, hablar de intimidad es hablar de sentimientos, de creencias (políticas, religiosas), pensamientos o de una información –como la clínica o la relativa a la vida sexual- cuya difusión puede producir ciertas reservas al individuo. Se trata en definitiva de aquellos datos que bajo ninguna circunstancia proporcionaría un individuo de manera libre y consciente.

Partiendo de este punto, nacen derechos como la inviolabilidad de las comunicaciones o el derecho a la propia imagen; ambos muy relacionados con la parte más privada de la psique del individuo.

3.2 ¿QUE ES LA PRIVACIDAD?

El diccionario de la Real Academia de la Lengua, define la privacidad como el "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*"

La privacidad, sin embargo, es un término más amplio que la intimidad: se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por si misma puede no ser relevante, pero que analizada en un momento o contexto concretos puede llevarnos a la construcción de un perfil muy fiable del individuo. Así, si al hablar de intimidad poníamos como ejemplos los sentimientos o creencias, podríamos ilustrar el concepto de privacidad con los libros que se consultan, las películas que se alquilan, las asociaciones a las que se pertenece, etc. Por sí solos, estos datos no tienen excesivo valor; ahora bien, tomados en conjunto, en un ambiente determinado, pueden hablarnos de los gustos del individuo, de sus preocupaciones o necesidades. En cualquier caso, sin llegar a esa zona reservada que define la intimidad.

Podríamos concluir que los asuntos íntimos son privados, pero que no todos los asuntos privados son íntimos. Hecha esta distinción, es el momento en el que entra en juego el derecho a la protección de datos de carácter personal, el cual se analiza en el punto 3.3; siguiente.

3.3 ¿QUE ES EL DERECHO FUNDAMENTAL A LA PROTECCION DE DATOS?

El derecho a la protección de datos viene consagrado en el artículo 18.4 de la Constitución Española de 1978 como uno de los derechos fundamentales de la persona, al establecer dicho artículo lo siguiente:

"*La Ley limitará el uso de la informática y la intimidad personal y familiar de los ciudadanos y del pleno ejercicio de sus derechos*"

No obstante además de la Constitución, el derecho fundamental a la protección de datos ha quedado consagrado en la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, que establece la definición y naturaleza de este derecho:
"El derecho fundamental a la protección de datos persigue garantizar a la persona "el poder de control sobre sus datos personales, sobre su uso destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado...)"

El objetivo de la protección de este derecho fundamental, no se reduce solo a los datos íntimos de la persona sino a cualquier dato de carácter personal sea o no intimo, cuyo conocimiento o tratamiento por un tercero pueda afectar a los derechos del individuo, sean o no fundamentales, porque su objeto no es solo la intimidad individual.

Por lo tanto, los poderes de disposición y control que tienen los individuos sobre sus datos personales se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, así como posible uso por un tercero ya sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a que uso lo está sometiendo, y, por otro, el poder de oponerse a esa decisión de uso.
De este modo la mencionada Sentencia dota de autonomía al derecho a la Protección de Datos de carácter personal, independizándole del derecho a la intimidad personal y familiar, consagrado en el artículo 18.1 de la Constitución.

Pero la realidad, es que, en la práctica, no puede hablarse de un límite exacto que delimite dónde empieza y acaba cada derecho; la protección de datos surge en cualquier tratamiento de información personal, sea del carácter que sea, y abarca tanto la esfera de lo íntimo como de lo privado. No se puede hablar objetivamente de intimidad y privacidad, pues son conceptos tan subjetivos que es cada individuo quien decide en cuál de las tres esferas coloca su información. Así, hay personas que prefieren exponer sus problemas de salud y hay otros que prefieren reservárselos. En cualquier caso, unos y otros son libres para manejar su información personal y, las garantías de un tratamiento de la información adecuado se lo ofrece el derecho a la protección de datos.

4 DATOS DE CARATER PERSONAL SUJETOS A LA LOPD Y SU REGLAMENTO

La LOPD es de aplicación en los siguientes supuestos:

1. Que existan datos de carácter personal; entendiendo como dato de carácter personal, a cualquier información sobre una persona que la identifique o la haga identificable. Es decir cualquier información que, de alguna manera se asocia a una persona física concreta es un dato de carácter personal. Por ejemplo, si tenemos como dato 18089710-S, simplemente es una secuencia de número y letras; si asociamos ese número como el DNI de una persona concreta, lo convertimos en un dato de carácter personal.

2. Que los datos de carácter personal, sean objeto de un tratamiento; es decir, atendiendo a la definición de tratamiento que se hace en a LOPD, cuando el dato es sometido a "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 decir, cualquier acción (incluso su mera conservación) que se haga con un dato, se considera tratamiento.

3. Que los datos se incorporen a un fichero; entendiendo fichero como un conjunto organizado de datos de carácter personal, independientemente de su forma o modalidad de creación, almacenamiento, organización y acceso que se tratan con una finalidad definida.

La protección de datos de carácter personal se refiere en concreto a los siguientes datos:

- ✓ **De carácter identificativos**: nombre, apellidos, dirección, NIF/CIF, teléfono, dirección electrónica, etc.

- ✓ **De carácter personal**: estado civil, fecha de nacimiento, edad, lugar de nacimiento, nacionalidad, sexo, etc.

- ✓ **De circunstancias sociales**: servicio militar, propiedades, aficiones, estilo de vida, pertenencia a clubes o asociaciones, etc.

- ✓ **Académicos o profesionales**: formación, titulación, historial de estudiante, experiencia profesional, etc.

- ✓ **Detalles de empleo**: profesión, puesto de trabajo, historial de la persona trabajadora, etc.

- ✓ **De información comercial**: actividades y negocios, licencias comerciales, suscripciones a publicaciones o medios de comunicación, etc.

- ✓ **Económico-financieros y de seguros**: ingresos, rentas, inversiones, préstamos, avales, datos bancarios, planes de jubilación, etc.

- ✓ **De transacciones**: transacciones financieras, indemnizaciones, etc.
- ✓ **Especialmente protegidos**: ideología, afiliación sindical, religión, creencias, salud, vida sexual, etc.

5 DATOS DE CARACTER PERSONAL EXLCUIDOS DE LA LOPD Y SU REGLAMENTO

El régimen de protección de datos de carácter personal **no será de aplicación** a los siguientes ficheros:

- ⇨ Los mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- ⇨ Los sometidos a la normativa sobre protección de materias clasificadas.
- ⇨ Los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

6 PRINCIPIOS DE LA PROTECCION DE DATOS

Estos principios han de regir todas las operaciones de tratamiento y cesión de datos de carácter personal.

6.1 CALIDAD DE LOS DATOS

6.1.1 Principio de calidad del dato con carácter general

La Ley tiende a establecer unos principios generales de calidad para garantizar un uso adecuado de los datos, de conformidad con los siguientes criterios:

a) Finalidad

Significa que los datos 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 los que se hayan obtenido.

Estos criterios de adecuación se relacionan expresamente con las finalidades para las que se han recabado los datos; en el caso que las finalidades del tratamiento cambien, los datos deberán ser cancelados. Por ejemplo, si recogemos datos para la participación en un concurso, dichos datos no los podremos destinar luego a finalidades distintas, diferentes o incompatibles.

b) Utilización no abusiva

La utilización no abusiva de los datos impide que los datos se usen para finalidades incompatibles o distintas con aquellas para las que hubiesen sido recogidos, si bien no se considera incompatible el tratamiento posterior de estos datos con fines históricos, estadísticos o científicos.

c) Exactitud

Significa que los datos tienen que ser exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Ello no significa que las empresas deban mantener exactos los datos cuando no tengan medios para conocer la exactitud/veracidad de los datos; pero, si tienen conocimiento de la inexactitud de un dato, deben proceder a actualizarlo.

Así, la corrección/actualización de los datos tratados puede realizarse:

- De oficio por el Responsable del Fichero, cuando conozca dicha inexactitud.
- A través del ejercicio del derecho de rectificación de los datos por el propio interesado.

En cuanto a datos recabados de fuentes accesibles al público (repertorios telefónicos, boletines oficiales, publicaciones) se mantiene esta obligación de exactitud y veracidad, pero hay que decir que no es responsabilidad del Responsable del Fichero comprobar si los datos

publicados en dichas fuentes son exactos o inexactos, aunque si se conociese la inexactitud debe procederse a actualizarlo.

d) Cancelación en caso de no necesidad

El art.4.5 dispone que –"*Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieren sido recabados o registrados*"-. Así, la conexión entre los datos y la finalidad que motivó su recogida se mantiene en todo momento. La cancelación se producirá directamente por el Responsable del Fichero en el momento en que el dato no sea necesario, sin perjuicio de la posibilidad que tiene el afectado de solicitar la cancelación del dato.

En el caso de que alguna obligación legal establezca la necesidad de conservar los datos una vez concluida la finalidad que motivó su recogida, el Responsable del Fichero podrá conservar los datos a través del boqueo del dato o previo proceso de disociación.

En cuanto al bloqueo de los datos, la LOPD establece, en el art. 16.3, que -"*La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante la prescripción de éstas. Cumplido el citado plazo deberá procederse a su supresión*"-.

El art. 16.5 establece que -"*Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado*"-.

En cuanto al procedimiento de disociación, podemos definirlo como todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable; en la práctica se traduce en la disociación de las tablas y campos que conforman el fichero, de manera que no son relacionables los datos o informaciones obtenidas con una persona identificada o identificable.

e) Almacenamiento

Los datos serán conservados de manera que peritan el ejercicio de los derechos de acceso, salvo que sean legalmente cancelados.

El derecho de acceso consiste en la facultad que tiene el afectado de solicitar y obtener, de manera gratuita y en un plazo determinado, la información sobre sus datos sometidos a tratamiento, las comunicaciones que se han realizado y las sesiones realizadas, principalmente. Este derecho será desarrollado con más profundidad en un apartado específico de esta Guía.

f) Lealtad

Se impone la prohibición de recoger los datos por medios fraudulentos, desleales o ilícitos.

6.2 CONSENTIMIENTO

6.2.1 Principio del consentimiento con carácter general

La LOPD establece una serie de limitaciones al tratamiento de los datos. Limitaciones fijadas para garantizar un uso adecuado, lícito, no excesivo y con las debidas medidas de seguridad que impidan la alteración, pérdida o tratamiento no autorizado de los datos.

Por tratamiento entiende la Ley –"*cualquier operación y procedimiento técnico de carácter automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*"-.

Al entender la Ley la necesidad del tratamiento, informatizado o no, de datos de carácter personal por parte de las empresas para poder desarrollar sus actividades propias, fija como contrapeso la necesidad de observar la voluntad del interesado.

En la mayoría de los supuestos, la voluntad se manifiesta a través del consentimiento y, en los casos en los que operan excepciones legales al consentimiento, el afectado manifiesta su voluntad a través de su derecho de oposición al tratamiento de los datos (como, por ejemplo, en el caso de datos procedentes de fuentes accesibles al público, donde no es necesario recabar el consentimiento previo del afectado para su tratamiento).

Además, fija para el tratamiento de los datos otras obligaciones básicas como son los principios de calidad de los datos, el derecho de información, las medidas específicas de los datos especialmente protegidos, las medidas de seguridad aplicables a los ficheros, el bloqueo y cancelación de los datos, la cesión de datos y el acceso a datos por cuenta de terceros.

Por último, la Ley utiliza un concepto amplio de tratamiento, englobando dos momentos importantes y que deben entenderse de forma separada: la recogida y el tratamiento en sí mismo de los datos.

6.3 DEBER DE INFORMACION

Las personas a las que se les solicita los datos personales deberán ser informadas de modo expreso, preciso e inequívoco:

- ✓ De la existencia del 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 formuladas.
- ✓ De las consecuencias de la obtención de 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 tratamiento.

6.4 DEBER DE SECRETO

Este deber de secreto debe ser adoptado por todo el personal laboral que accede a los Ficheros de datos. Además en las empresas, este deber fijado por la Ley se ve complementado por la obligación profesional de confidencialidad y secreto del Estatuto de las personas trabajadoras (descrita en el art.5.a) que se mantiene vigente hasta la finalización de la relación laboral.

Por ello, las obligaciones de Secreto, Confidencialidad y Custodia incumben a todo el personal y, de manera particular, a aquellos que en el desarrollo de sus funciones accedan a Ficheros que contienen datos personales.

En cumplimiento de estas obligaciones, las personas trabajadoras en plantilla de EHLABE. que traten o accedan a los Ficheros de datos de carácter personal no deberán ni podrán divulgar o comunicar a terceras personas la información o los datos que manejan o a los que tengan conocimiento en el desempeño de su cargo o funciones.

Además, para garantizar la Confidencialidad de la Información dentro de las entidades empresas y dada la importancia que la información y documentación tiene para la actividad ~~empresarial~~, el personal que acceda a los Ficheros de datos es recomendable que cumpla siempre con las siguientes medidas:

1. Deberá actuar siempre conforme a sus obligaciones profesionales de confidencialidad y secreto así como de acuerdo a lo dispuesto por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y su normativa de desarrollo.

2. El acceso a los datos personales contenidos en Ficheros únicamente se llevará a cabo por personal autorizado, limitado a las funciones y actividades a desempeñar.
3. No revelará información a personas ajenas que no deban tener acceso a dicha información.

6.5 DATOS ESPECIALMENTE PROTEGIDOS

Son datos que se refieren a aspectos personales e íntimos de la vida privada de las personas, por lo que merecen una mayor protección. Se pueden agrupar dichos datos en tres grupos en función de las especiales garantías que prevé la LOPD para su tratamiento.

6.5.1 Datos que revelen la ideología, afiliación sindical, religión y creencias

Son aquellos datos que puedan dar indicios sobre la ideología, la afiliación sindical, la religión y las creencias en general del individuo. Abarcará datos como la pertenencia a asociaciones, partidos políticos, la cuota sindical en la nómina, o la casilla correspondiente a la donación a la Iglesia Católica en la declaración del IRPF.

Cuando se pretenda recabar datos de este tipo en todo caso habrá que informar del contenido del artículo 16.2 de la Constitución que dispone que nadie pueda ser obligado a declarar sobre su ideología, religión o creencias. Como consecuencia de este precepto, el responsable del fichero tendrá que advertir al interesado de su derecho a no prestar su consentimiento.

Al estar ante el ejercicio de derechos fundamentales, la carga de la prueba recaerá sobre el responsable del tratamiento, por lo que se recomienda que tal información conste por escrito, por ejemplo, en el formulario de recogida junto con la cláusula de protección de datos.

Además, el tratamiento de dichos datos requiere haber recabado previamente el consentimiento expreso y por escrito del afectado. Este requisito se aplicará de la misma forma y con más fuerza cuando se quieran ceder los datos del interesado a un tercero.

Tratamiento de los datos: Queda prohibido crear un fichero con la finalidad exclusiva de tratar datos de carácter personal que revelen la ideología, afiliación sindical, religión o creencias. Eso significa que si bien se admite la posibilidad de tratar dichos datos, la finalidad tendrá que responder a un interés legítimo del responsable del fichero que en ningún caso podrá consistir en la creación de un fichero con esta finalidad exclusiva.
Excepciones: Ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro. Los ficheros de dichas entidades que tengan una finalidad política, filosófica, religiosa o sindical y que se refieran exclusivamente a datos relativos a sus miembros o asociados, están exentas de la obligación de recabar el consentimiento expreso y por escrito, previamente al tratamiento.

6.5.2 Datos que hagan referencia al origen racial, a la salud y a la vida sexual

Son aquellos datos que describen la raza del individuo, que describen la situación de la salud , como dolencias, enfermedades, altas y bajas en la empresa por enfermedad, historiales clínicos, datos de minusvalía en la nómina, etc. , y los descriptivos de las prácticas sexuales asimiladas por el afectado.

Solo podrán ser recabados, tratados y cedidos estos datos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

Tratamiento de los datos: 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 lo tanto siempre debe haber una razón legítima para el tratamiento de estos datos personales. Las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad. Por lo tanto, los centros como las clínicas privadas, que poseen el historial clínico de sus clientes, deberán ajustarse a este supuesto.
Excepciones: Tratamiento necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médicos, gestión de servicios médicos.

6.5.3 Datos relativos a comisión de infracciones penales o administrativas

Son aquellos datos que se refieran a cualquier infracción penal o administrativa de la que haya sido declarado culpable el interesado.

Tratamiento de los datos: Queda absolutamente prohibido para entidades privadas y queda reservado exclusivamente a las administraciones públicas competentes.

6.6 TRATAMIENTOS DE DATOS PERSONALES POR TERCEROS

6.6.1 Acceso a datos por cuenta de terceros

Se produce un acceso a datos por cuenta de terceros, cuando ~~SERMANFER SA~~. EHLABE recurre a una empresa externa para que realice el tratamiento de los datos, o cuando la prestación del servicio contratado implique o pueda implicar acceso a los sistemas y medios que contengan datos de carácter personal titularidad de EHLABE.

En este sentido desde el punto de vista de la Ley Orgánica de Protección de Datos, cada vez que EHLABE. externaliza un servicio, entran en juego dos factores: la necesidad de tratar información confidencial y los ficheros que contienen datos de carácter personal titularidad de EHLABE.

En este supuesto, existe un acceso a datos por cuenta de terceros en la que intervienen dos figuras:

- **Responsable del Fichero**: EHLABE. que contrata un servicio y es titular de los datos de carácter personal.
- **Encargado del Tratamiento**: empresa contratada por EHLABE. (el responsable del fichero) para llevar a cabo la prestación de un servicio en su nombre.

Por todo ello la **LOPD** exige que las relaciones entre el responsable y los diferentes terceros que realicen la prestación de un servicio para dicho responsable se han de regular por medio de un **contrato escrito** que incluya, de un modo específico, una Cláusula relativa a la protección de datos de carácter personal, en la que se deben incluir como mínimo los siguientes extremos:

- ✓ Relaciones que deben existir entre el Responsable y el Encargado del Tratamiento.
- ✓ Las condiciones que deben ponerse en práctica y en conocimiento del Responsable para la subcontratación por parte del Encargado del Tratamiento del servicio o parte del servicio que presta.
- ✓ Las Obligaciones en cuanto a la conservación de los datos una vez cumplida la prestación del servicio.

- ✓ Las Obligaciones en cuanto a las Medidas de Seguridad de obligado cumplimiento a poner en práctica en correspondencia con el alcance del tratamiento y al nivel de los datos tratados.

En la relación con Terceros (proveedores de servicios) el acceso a datos por parte de un Encargado del Tratamiento no se considera una cesión o comunicación de datos, siempre que se cumpla con lo establecido en el art. 12 de la Ley Orgánica 15/1999 del 13 de Diciembre.

En cumplimiento de los dispuesto en el **Articulo 12 de la Ley Orgánica 15/1999 de Protección de Datos**, todos los contratos de prestación de servicios que conlleven la posible explotación, uso o acceso a datos personales responsabilidad de EHLABE. deben estar regulados por una Cláusula que refleje un compromiso de confidencia por parte del proveedor en cumplimiento de la normativa de protección de datos.

6.6.2 Cesión de datos personales

Se entiende por cesión o comunicación de datos toda revelación de datos personales realizada a una persona física o jurídica distinta al interesado.

Para que la cesión de datos personales se lleve a cabo de conformidad con LOPD y su reglamento de desarrollo es necesario que con carácter previo a la cesión o comunicación de datos se informe al interesado de:

- ✓ la posibilidad de la cesión a fin de que preste su consentimiento, y
- ✓ de la finalidad del tratamiento de los datos de carácter personal

No obstante no será necesario el consentimiento del afectado cuando:

- ➢ La cesión o comunicación de datos este autorizada por una ley. Es el caso por ejemplo, de la cesión o comunicación de de datos que se realiza a la Seguridad Social para el cumplimiento de las obligaciones laborales
- ➢ Cuando se trate de datos recogidos de fuentes accesible al público

6.6.3 Criterios diferenciadores entre acceso a datos por cuenta de terceros y cesión de datos

ACCESO A DATOS **POR CUENTA DE 3º**	➢ La actividad del Encargado del Tratamiento se limita a prestar un servicio al Responsable. ➢ El poder de decisión sobre el tratamiento de los datos solo recae sobre el Responsable del Fichero.
CESION DE DATOS	➢ El cesionario de los datos no presta un servicio para el Responsable del Fichero. ➢ El cesionario tiene poder de decisión sobre el tratamiento de los datos, se convierte en un nuevo Responsable del Fichero.

6.7 MEDIDAS DE SEGURIDAD

Desde el punto de vista de la Ley Orgánica de Protección de Datos, las medidas de seguridad van destinadas a todas las organizaciones, empresas e instituciones que almacenan y tratan datos de carácter personal en sus sistemas de información, siendo su finalidad principal proteger los datos de carácter personal tratados de posibles incidencias que puedan provocar su pérdida, alteración u acceso no autorizado (tanto interno como externo).

Por ello, la adopción de medidas técnicas y organizativas tendentes a garantizar la seguridad de los datos de carácter personal es una obligación básica que debe ser cumplida por todas las empresas que traten, almacenen y accedan a datos de carácter personal. Medidas que deberán adoptarse en función del nivel de los datos almacenados/tratados, de la estructura y organización de la empresa y del estado de la tecnología.

Así, podemos observar que la normativa fijada para ofrecer unos mínimos de seguridad en el tratamiento de los datos de carácter personal, busca el ofrecer unas directrices de seguridad informática que pueden ser adoptadas e implantadas en todas las empresas, independientemente de su tamaño y organización. Un concepto de protección de la información como activo empresarial considerando a la información como elemento relevante para mejorar la competitividad, la rentabilidad y el cumplimiento de los fines empresariales conjugada con la protección del derecho a la intimidad de las personas.

7 DERECHOS DE LOS PERSONAS CIUDADANOS

Los derechos que vamos a enumerar nacen para garantizar a los personas ciudadanos las posibles intromisiones en la intimidad u honor como consecuencia del uso de la informática:

- Derecho de **acceso**. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas.

- Derecho de **rectificación y cancelación**. El Responsable del Tratamiento tiene la obligación de rectificar o cancelar aquellos datos de carácter personal que resulten inexactos, incompletos o que no se ajusten a lo dispuesto en la Ley 15/1999, en el plazo de diez días a contar desde que el interesado ejerce el derecho.

- Derecho a **impugnar valoraciones** de su comportamiento basadas en el tratamiento de datos personales.

- Derecho de **consulta el Registro General de Protección de Datos**. Cualquier persona puede conocer la existencia de tratamientos de datos personales, sus finalidades y la identidad del responsable del mismo.

- Derecho a **indemnización**.

7.1 DERECHOS ARCO

Nos referimos a los derechos de Acceso, Rectificación, Cancelación y Oposición respecto del tratamiento de datos personales y son conocidos como los derechos ARCO. Se trata de unos derechos personalísimos, esto es, sólo pueden ser ejercidos por el afectado o su representante legal.

Su ejercicio está regulado en los artículos 15 y siguientes de la LOPD y en la Instrucción 1/1998 de la AEPD.

a) Derecho de Acceso

El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

- **Justificación:** no es necesaria, salvo si se ha ejercitado el derecho en los últimos doce meses.

- **Plazo:** El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. El acceso podrá hacerse efectivo durante 10 días hábiles tras la comunicación de la resolución.

- **Denegación:** debe motivarse e indicar que cabe invocar la tutela de la AEPD. Son motivos de denegación que el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud (salvo que se acredite un interés legítimo al efecto) y que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de sus datos.

b) Derecho de Rectificación

Derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

- **Justificación:** debe indicarse a qué datos se refiere y la corrección que haya de realizarse aportando documentación.
- **Plazo:** 10 días hábiles.
- **Denegación:** debe motivarse y procede indicar que cabe invocar la tutela de la AEPD.

c) Derecho de Cancelación

Derecho del afectado a que se supriman los datos que resulten ser inadecuados o excesivos.

- **Justificación**: debe indicarse el dato a cancelar y la causa que lo justifica, aportando documentación.
- **Plazo**: 10 días hábiles.
- **Denegación**: debe motivarse y procede indicar que cabe invocar la tutela de la AEPD. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

d) Derecho de Oposición

Derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los supuestos en que no sea necesario su consentimiento para el tratamiento, que sea tratamiento de ficheros de prospección comercial o que tenga la finalidad de adoptar decisiones referidas al interesado y basadas únicamente en el tratamiento automatizado de sus datos.

- **Justificación:** concurrencia de motivos fundados y legítimos relativos a su concreta situación personal.
- **Plazo:** 10 días hábiles.
- **Denegación:** debe motivarse e indicar que cabe invocar la tutela de la AEPD.

7.2 ESPECIALIDAD EN EL FICHERO DE VIDEOVIGILANCIA

El ejercicio de los derechos posee perfiles específicos en el ámbito de la videovigilancia.

En primer lugar, no resulta posible el ejercicio del derecho de rectificación ya que por la naturaleza de los datos -imágenes tomadas de la realidad que reflejan un hecho objetivo- se trataría del ejercicio de un derecho de contenido imposible.

Por otro lado, el ejercicio del derecho de oposición también plantea enormes dificultades. Si este se interpreta como la imposibilidad de tomar imágenes de un sujeto concreto en el marco de instalaciones de videovigilancia vinculadas a fines de seguridad privada no resultaría tampoco posible su satisfacción en la medida en la que prevalecería la protección de la seguridad.

Por otra parte el ejercicio del derecho de acceso reviste características singulares:

- Requiere aportar como documentación complementaria el aportar una imagen actualizada que permita al responsable verificar y contrastar la presencia del afectado en sus registros.
- Resulta prácticamente imposible acceder a imágenes sin que pueda verse comprometida la imagen de un tercero. Por ello puede facilitarse el acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.
- Si se ejerciese el **derecho de acceso** ante el responsable de un sistema que únicamente reproduzca imágenes sin registrarlas deberá responderse en todo caso indicando la ausencia de imágenes grabadas.
- La cancelación solicitada por el afectado se rige por lo previsto en la LOPD sin especialidad alguna.
- No debe olvidarse que conforme a las previsiones del RDLOPD en caso de denegación de un derecho deberá indicarse expresamente la posibilidad de reclamar su tutela ante el Director de la Agencia Española de Protección de Datos.

Es aconsejable consultar la Guía del responsable de ficheros disponible en el Canal de Documentación del website de la Agencia:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

8 LAS MEDIDAS DE SEGURIDAD

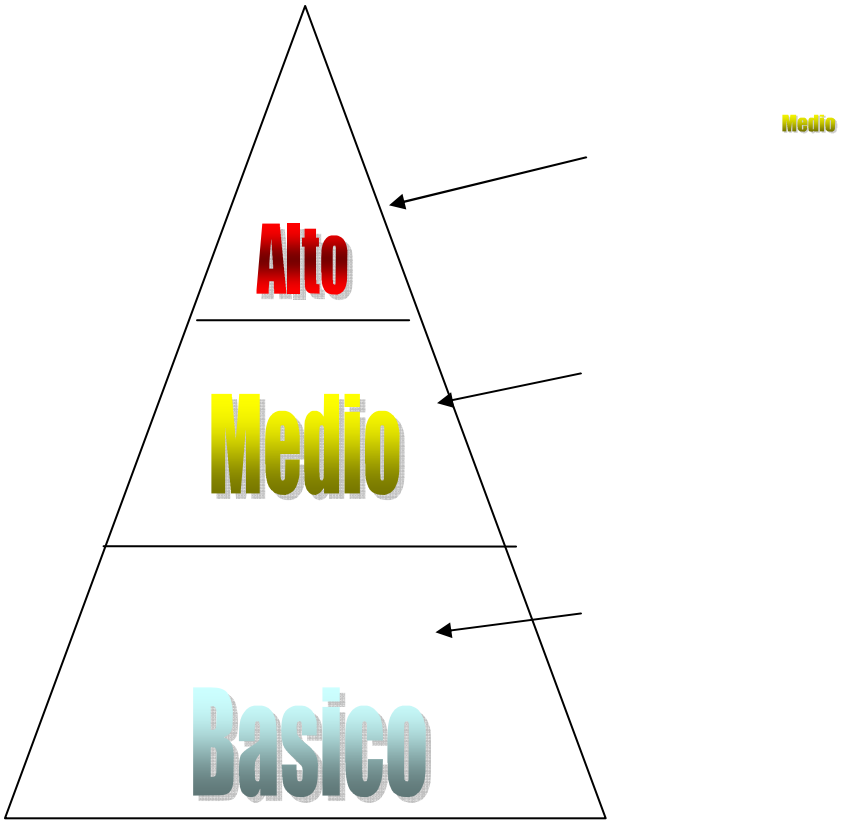
Los derechos y obligaciones que se describen en la normativa española de protección de datos son de tres tipos:

1. **Jurídicos**: son los derechos y deberes que se recogen en la LOPD y su objetivo es garantizar que cada persona es dueña de su información.

2. **Organizativos**: se trata de procedimientos de seguridad que se regulan en el RD 1720/2007 encaminados a proporcionar una mayor seguridad de la información y a que los profesionales que tratan datos de carácter personal lo hagan cumpliendo los deberes de sigilo y reserva.

3. **Tecnológicos**: también se regulan en el RD 1720/2007 y buscan garantizar una mayor seguridad de la información dotando a los sistemas de información y a los tratamientos en soporte papel de medidas que eviten su pérdida o fuga.

Pues bien, las medidas organizativas y tecnológicas son más gravosas cuanto más sensible es la información que se trata. De esta forma, existen tres niveles distintos de seguridad en función de la información que se trata:



Nivel Básico

Se entiende por ficheros de nivel básico todos los ficheros que, por defecto, no se pueden calificar de nivel medio o alto. A estos efectos, establece que todos los ficheros que contengan datos de carácter personal han de adoptar las medidas de seguridad calificadas como de nivel básico.

Las medidas de seguridad del nivel básico son las medidas que obligatoriamente deberán adoptarse para proteger la confidencialidad e integridad de cualquier fichero que contenga datos de carácter personal.

Las medidas de seguridad de nivel básico son las siguientes:

a) **Tratamientos Automatizados (soporte informático**)

- Funciones y obligaciones del personal → Todo el personal que trate datos personales debe conocer sus funciones y obligaciones respecto del tratamiento del mismo.
- Registro de incidencias → Debe crearse un registro de incidencias que anote cualquier problema en el que pueda verse afectada la seguridad de los datos personales.
- Control de acceso → Cada usuario del sistema de información sólo podrá acceder a la información que necesite para su trabajo.
- Gestión de soportes y documentos → Debe existir un control de entrada y salida de soportes informáticos (pendrives, Cds, etc) con datos personales.
- Identificación y autenticación → Cada usuario del sistema de información deberá tener su usuario y contraseña de acceso personalizada y debe cambiarse periódicamente.
- Copias de respaldo y recuperación → se deben realizar copias de seguridad al menos semanalmente.

b) **Tratamientos No Automatizados (soporte Papel)**

- Criterios de archivo → La información debe archivarse de manera que permita su conservación y su fácil localización y acceso.
- Dispositivos de almacenamiento → La documentación, mientras no esté en tratamiento, debe almacenarse en dispositivos con llave o control de apertura y acceso.
- Custodia de los soportes → durante el tratamiento efectivo de la información debe mantenerse de manera que no sea accesible por terceros.

Nivel Medio

Son considerados como ficheros de nivel medio, los ficheros que contengan datos relativos a:

- ✓ Comisión de infracciones administrativas o penales→ sólo las Administraciones Públicas pueden tratar datos relativos a la comisión de infracciones administrativas o penales.

- ✓ Hacienda Pública→ hace referencia a los ficheros cuya titularidad corresponda a la Hacienda Pública, debiendo entenderse como aplicable a aquellos ficheros cuyo responsable sea una Administración Pública que ostente potestades en materia tributaria.

- ✓ Servicios financieros→ Los datos sobre transacciones económico- financieras cuando constituyan un" servicio financiero" conforme a la definición dada por la Agencia de Protección de Datos y que se refiere a las actividades de las entidades de crédito, de las compañías de seguros y de las empresas de inversiones.

- ✓ Ficheros de solvencia patrimonial→ aquellos ficheros cuyo funcionamiento se rige por el artículo 29 de la LOPD referido a la "prestación de servicios de información sobre solvencia patrimonial".

- ✓ Ficheros→ que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo: no se deben implantar, además de las medidas de seguridad de nivel básico, todas las medidas de nivel medio, sino únicamente la obligación de someter los sistemas de información a una Auditoría al menos cada dos años: la implantación de un mecanismo de identificación de forma inequívoca y personalizada y la limitación de intentos de acceso fallidos; el control de acceso físico y el sistema de registro entrada y salida de soportes, de destrucción de soportes y protección de los datos contra cualquier recuperación indebida cuando salen de los locales.

- ✓ Los ficheros considerados como de nivel medio requieren la aplicación de las medidas de seguridad de nivel básico, además de las nivel medio.

Las medidas de seguridad de nivel medio son las siguientes:

a) Tratamientos Automatizados (soporte informático)

- Responsable de seguridad → deberá designarse, al menos una persona, encargada de velar por el cumplimiento de las normativas de seguridad y LOPD.

- Auditoría → al menos cada dos años, los sistemas de información deben someterse a una auditoria que verifique el cumplimiento.

- Medidas adicionales de gestión de soportes y documentos.

- Medidas adicionales de identificación y autenticación.

- Control de acceso físico → las salas donde se ubiquen los sistemas de información deberán controlar los accesos.

- Medidas adicionales del registro de incidencias.

b) Tratamientos No Automatizados (soporte Papel)

- Responsable de seguridad → deberá designarse, al menos una persona, encargada de velar por el cumplimiento de las normativas de seguridad y LOPD.
- Auditoría → al menos cada dos años, los tratamientos en papel deben someterse a una auditoria que verifique el cumplimiento.

Nivel Alto

Son considerados como ficheros de nivel alto, es decir, requieren la aplicación tanto de las medidas de seguridad de nivel básico como las de nivel medio y las de nivel alto, los ficheros que contengan datos relativos a:

- ✓ Ideología
- ✓ Creencias
- ✓ Origen racial
- ✓ Salud
- ✓ Vida sexual
- ✓ Datos recabados para fines policiales sin consentimiento
- ✓ Datos de afiliación sindical
- ✓ Religión
- ✓ Datos relacionado con la violencia de Género

Las medidas de seguridad de nivel medio son las siguientes:

a) **Tratamientos Automatizados (soporte informático)**

- Medidas adicionales de gestión de soportes y documentos.
- Medidas adicionales a las copias de respaldo y recuperación.
- Registro de accesos → las aplicaciones sobre las que se traten los datos de nivel alto deben permitir conocer quién ha accedido, cuándo, si ha modificado o no los registros.
- Telecomunicaciones → la transmisión de datos de carácter personal a través de redes de comunicaciones electrónicas se realizará cifrando datos o bien

utilizando cualquier mecanismo que garantice que la información no sea accesible por terceros.

b) **Tratamientos No Automatizados (soporte Papel)**

- Almacenamiento de la información → la documentación con datos de nivel alto debe estar en archivos de acceso restringido.
- Copia o reproducción → deberán establecerse mecanismo de control de copias y de destrucción de papel.
- Acceso a la documentación → los accesos al archivo deberán ser controlados y autorizados.
- Traslado de documentación → para el traslado de documentación con datos de nivel alto debe hacerse de manera que no sea accesible por terceros.

9 INFRACCIONES Y SANCIONES

9.1 TIPOS DE INFRACCIONES

La Ley 2/2011, de 4 de marzo, de Economía Sostenible, (disposición final quincuagésima), modifica el Titulo VII de la Ley Orgánica 15/1999, relativa a procedimiento sancionador mediante la cual se amplían los criterios de modulación y adecuación de las infracciones, las cuales quedan redactadas de la siguiente manera:

a) Infracciones LEVES

- No inscribir los ficheros ante el Registro del AEPD.
- La recogida de datos de carácter personal sin informar al afectado acerca del tratamiento de sus datos.
- La transmisión de datos a un encargado de tratamiento sin dar cumplimiento a los deberes formales establecidos en el Art. 12 de la LOPD.

SANCION: entre 900 € y 40.000 €

b) Infracciones GRAVES

- El impedimento u obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
- Tratar o recoger datos sin el consentimiento expreso del afectado cuando sea necesario conforme a lo dispuesto en la Ley.
- La vulneración del deber de guardar secretos acerca del tratamiento de los datos de carácter personal.
- El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos cuando no se hayan recabada del propio interesado.
- Mantener ficheros o equipos informáticos sin las condiciones de seguridad correspondientes.
- Obstruir el ejercicio de la función inspectora de la AEPD.

SANCION: entre 40.001 € y 300.00 €

c) Infracciones MUY GRAVES

- La recogida de datos en forma engañosa o fraudulenta.
- Comunicar o ceder datos fuera de los casos permitidos legalmente.
- No cesar en el uso ilegítimo de los datos cuando haya un requerimiento por parte de la AEPD.
- La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de seguridad equiparable sin autorización del Director de la AEPD salvo en los supuestos autorizados legalmente.

SANCION: entre 300.001 € y 600.000 €

9.2 MEDIDAS QUE PUEDE DICTAR LA AGENCIA ESPAÑOLA DE PROTECCION DE DATOS

- Requerimiento para la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la Ley.
- Ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando la empresa no se ajuste a sus disposiciones.
- Inmovilización de los ficheros o tratamientos de datos y cesación en la utilización o cesión ilícita de los datos.

10 MEDIOS DE OBTENCION DE DATOS DE CARACTER PERSONAL

10.1 CUESTIONARIOS IMPRESOS

En cumplimiento del deber de información anteriormente mencionado en el punto 4.3 de este manual, *"cuando se utilicen cuestionarios u otros tipos de impresos, figurarán en los mismos, en forma clara y legible, los siguientes avisos:*

- ✓ *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.*
- ✓ *Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean 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 tratamiento o, en su caso, de su representante."*

Recomendamos diferenciar los campos obligatorios de los campos voluntarios, incluyendo una casilla que permita al cliente manifestarse sobre la cesión de sus datos.

10.2 CORREO ELECTRONICO (E-MAIL)

Se recomienda en cumplimiento del deber de información (art.5 LOPD) incluir un aviso legal al final de la firma del emisor del correo para que todas las personas que accedan a él o respondan con sus datos, conozcan que sus datos van a ser incluidos en un fichero y de dónde pueden ejercer sus derechos de acceso rectificación, oposición y cancelación de sus datos personales.

10.3 OBTENCION DE DATOS POR TELEFONO

Para la inclusión de datos personales enviados por medios telefónicos habrá que tomarse las mismas precauciones que en cualquiera de los medios anteriormente citados. Si los datos se recaban por teléfono de nuevo estamos en la obligación se debe informar al afectado:

- ✓ *"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.*
- ✓ *Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean 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 tratamiento o, en su caso, de su representante.*

- ✓ *De la cesión a terceras empresas"*

Estos deberes deberán estar documentados en procedimientos o en el Documento de Seguridad para que la persona que capte los datos mediante el teléfono pueda informar debidamente al afectado.

Si lo que se recoge es el consentimiento del afectado para tratar sus datos con nivel de protección alto, se deberá grabar dicha aceptación específica y explícita del afectado y guardarse, ya que tendrá el mismo nivel probatorio que si se hubiera recogido por escrito.

10.4 PAGINAS WEB

En las páginas web se deberá incluir un aviso legal que informe adecuadamente al usuario de la política de protección de datos del responsable del fichero y del ejercicio de sus derechos.

Igual que en los casos previstos en los puntos anteriores "*cuando se recaben datos personales a través de una página web, se informará previamente al usuario, de forma clara e inequívoca, de los siguientes extremos":*

- ✓ *La existencia de un fichero o tratamiento de datos de carácter personal, finalidad de la recogida y destinatarios de la información.*

- ✓ *Inscripción del fichero en el Registro de la Agencia de Protección de Datos.*

- ✓ *Carácter obligatorio o facultativo de la respuesta a las preguntas que en su caso les sean planteadas, así como de las consecuencias de la obtención de los datos o la negativa a suministrarlos.*

- ✓ *Posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.*

- ✓ *Identidad y dirección del responsable del tratamiento de los datos.*

- ✓ *De la cesión a terceras empresas*

Además, se deben incluir en la política de privacidad los siguientes extremos:

- ✓ El usuario será el único responsable de cumplimentar los formularios con datos falsos, inexactos, incompletos o no actualizados.

- ✓ Cualquier cesión a terceros de los datos personales de los usuarios de este portal, será comunicada debidamente a los afectados especificando la identidad de los cesionarios y la finalidad con que se van a tratar los datos que se cedan.

11 TRATAMIENTOS CON FINES DE PUBLICIDAD Y DE PROSPECCION COMERCIAL

La LOPD y la reciente aprobación del RLOPD ha supuesto un cambio en la forma de plantear las campañas publicitarias por parte de las empresas a clientes y potenciales clientes a la vista de las restricciones y limitaciones impuestas por dicha normativa, especialmente en lo que respecta al marketing positivo.

11.1 TRATAMIENTO CON NATURALEZA PUBLICITARIA

Cualquier actividad relacionada con la promoción de un producto o servicio que implique el tratamiento de datos de carácter personal debe ajustarse a las especificaciones contenidas en la LOPD. En este sentido la mencionada ley LOPD considera que tienen una naturaleza publicitaria todos aquellos tratamientos que se efectúen con las siguientes finalidades:

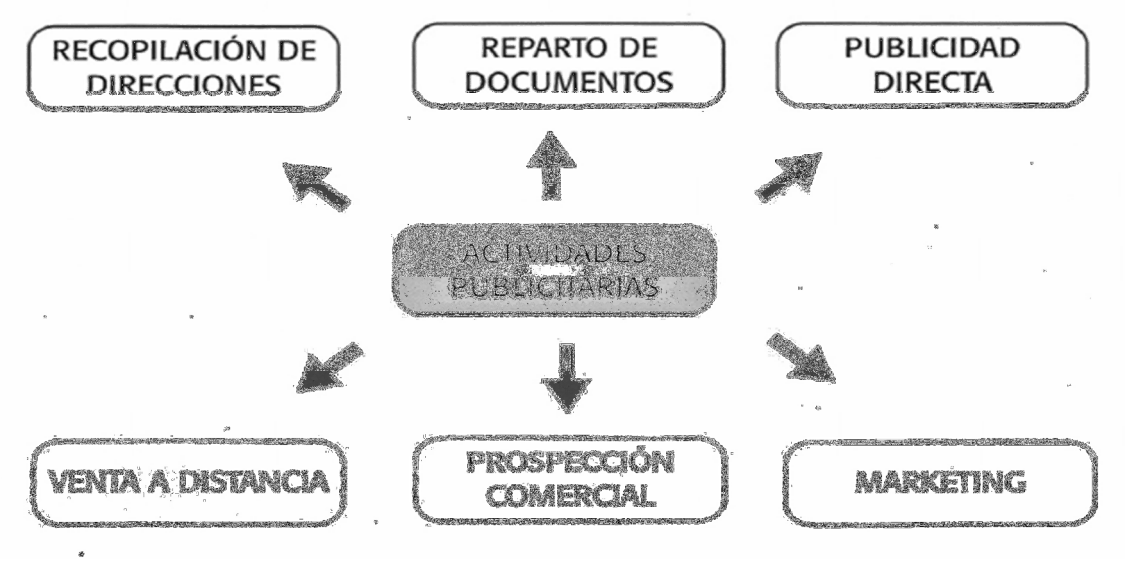
- Recopilación de direcciones con fines comerciales
- Publicidad directa
- Venta a distancia
- Prospección comercial, marketing y otras actividades análogas
- Remisión de documentos comerciales

Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar tanto sus propios productos o servicios, como los de terceros, sólo podrán utilizar nombres y direcciones o cualquier otro dato personal cuando los mismos se encuentren en uno de los siguientes casos:

- ✓ Figuren en alguna de las FUENTES ACCESIBLES AL PUBLICO a las que se refiere la LOPD y el RLOPD y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas anteriormente.
- ✓ Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

La AEPD considera nulo el consentimiento obtenido genéricamente para fines de publicidad, marketing o prospección comercial, debiendo indicar específicamente el tipo de publicidad y el sector de la misma.

Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de sus datos, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, con la simple solicitud, y no remitiéndose más comunicaciones en el futuro.



11.2 FUENTES ACCESIBLES AL PÚBLICO

Son fuentes accesibles al público aquellos ficheros 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.

Es decir, para que un fichero sea considerado como fuente de acceso público es preciso que su acceso sea libre con o sin pago de un precio a cambio.

Las fuentes de acceso público tienen una enorme trascendencia ya que la LOPD permite, en estos supuestos, legitimar tanto el tratamiento de los datos, como las cesiones de éstos, sin necesidad de recabar el consentimiento del afectado. Cualquier dato que provenga de una fuente no accesible al público no podrá ser tratado para finalidades de publicidad y prospección comercial, a no ser que cuente con el consentimiento informado del interesado.

Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, el responsable deberá informar al interesado en cada comunicación que se le dirija:

- ✓ Del origen de los datos, es decir, que sus datos han sido obtenidos de fuentes accesibles al público.
- ✓ De la identidad del responsable del tratamiento.
- ✓ De la entidad, en su caso, de la que se hubieran obtenido.
- ✓ De los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

Por todo ello y en cumplimiento de este deber de información se garantiza que el interesado no quede indefenso. Al ser informado del tratamiento podrá ejercer, si lo estima conveniente, sus derechos de acceso, rectificación, cancelación u oposición, recomendamos la inclusión del siguiente aviso legal:

EJEMPLO DE AVISO LEGAL

En cumplimiento de la Ley orgánica de Protección de datos de carácter personal, le informamos que la mercantil_____, con CIF número _____, y con domicilio social en la calle_____, a obtenido sus datos de carácter personal de la fuente accesible al público denominada_____.

Ejercicio de sus derechos: En los términos y con los requisitos previstos en la normativa sobre protección de datos vigentes, Vd. podrá ejercitar los derechos de acceso, rectificación, cancelación u oposición, respecto de los datos personales, a la dirección anteriormente mencionada.

Tienen el carácter de fuentes accesibles al público:

a) El censo promocional

Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, compuesto por los datos de nombre, apellidos y domicilio que constan en el censo electoral (datos de empadronamiento).

El uso de cada lista del censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público, debiendo proceder a solicitar una nueva copia.

Los interesados podrán solicitar no aparecer en el censo promocional mediante un procedimiento gratuito y en el que la entidad responsable deberá prestar especial atención a los plazos dispuestos por la normativa para la atención de dicha solicitud de cancelación u oposición, existiendo únicamente 10 días respecto de las informaciones que se realicen mediante consulta o comunicación telemática.

El censo promocional se realizado anualmente por parte del Instituto Nacional de Estadística con la única finalidad de reducir el tráfico ilegal de datos personales entre las empresas de publicidad y marketing directo.

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, establece la “digitalización” completa de todos los procesos de la Administración Pública, por lo que el censo promocional se encuentra actualmente digitalizado, resultando de especial interés para el responsable de protección de datos de una entidad tener en cuenta que en el caso de que se obtenga telemáticamente una copia de la lista en formato

electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

Igualmente, es necesario tener en cuenta que según el propio Instituto Nacional de Estadística, trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

b) Las guías de servicios de comunicaciones electrónicas (repertorios telefónicos)

Cada repertorio telefónico es considerado fuente accesible al público hasta que se publique una nueva edición, lo que ocurre cada año, por lo que los repertorios anteriores pierden ese carácter y para tratar los datos allí contenidos es necesario, como regla general, obtener el consentimiento del titular del dato.

La LOPD señala, a este respecto, que los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica, es decir, por la Ley General de Telecomunicaciones 32/2003, de 3 de noviembre, y su normativa de desarrollo, en particular el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

La Ley General de Telecomunicaciones regula el derecho de los abonados a:

- Un servicio telefónico disponible al público.
- Una guía general de números de abonados, ya sea impresa o electrónica, o ambas.
- Que se actualice, como mínimo, una vez al año.
- Que se ponga a disposición de todos los usuarios finales de dicho servicio, incluidos los usuarios de teléfonos públicos de pago, al menos un servicio de información general sobre números de abonados.

Todos los abonados al servicio telefónico disponible al público tendrán derecho a figurar en la mencionada guía general (guía telefónica), sin perjuicio, en todo caso, del respeto a las normas que regulen la protección de los datos personales y el derecho a la intimidad, es decir, sin perjuicio del derecho a solicitar que sus datos no aparezcan.

Respecto a las guías telefónicas, el Real Decreto 424/2005 establece que los operadores deberán informar gratuitamente a sus abonados, antes de incluir sus datos en cualquier tipo de guía de abonados, de la finalidad de dicha guía, así como de cualquier otra posibilidad de uso basada en funciones de búsqueda incorporadas en sus versiones electrónicas.

Asimismo requiere que el operador obtenga el consentimiento expreso del abonado para su inclusión en la guía. Si el abonado no hubiese dado su consentimiento expreso, se entenderá que no acepta que se publiquen en la guía correspondiente sus datos.

Los abonados tendrán derecho a que sus datos que aparezcan en la guía no sean utilizados con fines de publicidad o prospección comercial y a que así conste de forma clara en la guía. Del mismo modo, tendrán derecho a que se omita parcialmente su dirección o algún otro dato, en los términos que haya estipulado su proveedor.

Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique. En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

Con esto se pretende asegurar que los datos personales sean actualizados y respondan a la situación real del interesado. Perdido el carácter de fuente accesible al público, será necesario recabar el consentimiento del afectado para el tratamiento de sus datos.

c) Las listas de personas pertenecientes a grupos de profesionales

Tienen la consideración de fuentes accesibles al público las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios Profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

Si la guía profesional contiene otros datos (por ejemplo, la dirección de correo electrónico), no podrá tener la consideración de fuente accesible al público, ya que los datos exceden de los enumerados en la LOPD.

Los ficheros que conteniendo los datos enumerados sean utilizados internamente por el Colegio Profesional o sean de acceso restringido, por ejemplo, a los propios colegiados, no tendrán la condición de fuente accesible al público y, por tanto, no podrán ser utilizados para el envío de comunicaciones comerciales sin el consentimiento previo del usuario.

Los grupos profesionales pueden publicar las listas de sus miembros sin necesidad de recabar el consentimiento del interesado, siempre que los datos que figuren en estas listas se limiten a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por parte de los responsables del mantenimiento de dichas fuentes requiere el consentimiento del afectado, que puede revocarlo en cualquier momento.

Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios Profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial**,** debiendo atenderse dicha solicitud en el plazo de 10 días, respecto de las informaciones que se realicen mediante consulta o comunicación telemática, y en la siguiente edición del listado cualquiera que sea el soporte en el que se edite.

Este régimen no es aplicable a la utilización de ficheros de colegiados por los propios colegios profesionales con fines de publicidad y prospección comercial, por ser ficheros propios, es decir, los colegios profesionales podrán utilizar los datos personales de sus miembros con fines de publicidad y prospección comercial, únicamente si el envío tiene una relación directa con el ejercicio profesional o si ha recabado previamente el consentimiento del interesado.

Un Colegio profesional no puede ceder los datos de sus colegiados a una entidad aseguradora para que ésta pueda utilizarlos en una campaña de promoción de un determinado producto asegurador que no tenga relación directa con su actividad profesional. Sin embargo, un Colegio profesional de abogados, por ejemplo, está capacitado para ceder una base de datos completa de sus colegiados a una editorial jurídica, para que ésta la pueda utilizar para remitir publicidad a los colegiados de una base de datos online de legislación y jurisprudencia.

d) Los diarios y **boletines oficiales**

Así, por ejemplo, el Boletín Oficial del Estado, los boletines de las distintas Comunidades Autónomas o el Boletín Oficial del Registro Mercantil tienen el carácter de fuente accesible al público.

Sin embargo, los datos contenidos en registros públicos, como el Registro Mercantil o el de la Propiedad, o en los tablones de los juzgados, no tienen esta consideración.

e) Los medios de comunicación social

Son fuentes de acceso público los datos que sean difundidos a través de prensa, radio y televisión, no obstante no existe actualmente ninguna definición legal de “medios de comunicación social’ por lo que se plantean diferentes cuestiones, tales como, si un Blogs podría llegar a ser considerado un medio de comunicación social.

La definición de fuente accesible al público dada por la LOPD es taxativa respecto a los elementos que la contienen, lo que impide que se considere a las páginas web como fuentes accesibles al público (dado que no aparece expresamente referenciada). Por ello, para tratar la información contenida en dichas páginas debería obtenerse el consentimiento de los afectados.

No obstante, y a pesar del criterio mantenido por la AEPD, en su Informe Jurídico respecto a Internet, considerando a éste como un canal de comunicación y no como medio de comunicación social, es probable que determinados sitios web (no Internet en general) en un futuro cercano y más aún, cuando los propios medios de comunicación tradicionales están tendiendo a la digitalización de sus ediciones y programaciones, pasen a ser considerados medios de comunicación social y, por tanto, puedan ser utilizados sus datos de forma legítima.

11.3 CAMPAÑAS PUBLICITARIAS

11.3.1 Realizadas por el responsable

Como regla general, es preciso contar con el consentimiento inequívoco del afectado. No obstante, es posible que el responsable del fichero se dirija al afectado cumpliendo con su obligación de información concediéndole un plazo de 30 días para manifestar su negativa al tratamiento y advirtiéndole de que, en caso de no pronunciarse a tal efecto, se entenderá que consiente el tratamiento de sus datos de carácter personal.

La carga de la prueba de la obtención del consentimiento recae sobre el Responsable del Tratamiento, siendo necesario que éste pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso, no puede proceder al tratamiento de los datos.

Tanto si se realizó a través de medios automatizados, como si se hizo a través de formularios en papel, es necesario que el responsable del fichero cuente con una copia o, en su caso, con algún dispositivo técnico que permita acreditar que el usuario, en una fecha concreta, cumplimentó el formulario correspondiente, aceptando la casilla de recepción de comunicaciones comerciales en cuestión.

Para que EHLABE. pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes será preciso que disponga del consentimiento inequívoco de los mismos, o que el tratamiento se ampare en alguna excepción legal contemplada en la LOPD.

11.3.2 Realizadas por un tercero

La actividad de publicidad y prospección comercial frecuentemente es subcontratada a empresas dedicadas a esta finalidad, lo cual provoca a menudo situaciones complejas en las que puede resultar difícil determinar quién es el responsable del tratamiento y del cumplimiento de las obligaciones en materia de protección de datos.

En caso de que EHLABE contrate a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas:

- Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por EHLABE., ésta será responsable del tratamiento de los datos.
- Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsables del tratamiento.
- Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

Se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

En estos casos, EHLABE deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la normativa sobre protección de datos.

El supuesto más frecuente de campañas realizadas por un tercero es el siguiente: una empresa desea lanzar una campaña de publicidad segmentando el público objetivo al que se va a dirigir. En lugar de llevarla a cabo ella misma, contrata esta actividad a otra empresa que dispone de una gran base de datos debidamente sectorizada. En ocasiones, intervienen otras entidades, como la encargada del ensobrado de la publicidad o aquella que realiza el envío o mailing.

11.4 LLAMADAS TELEFONICAS NO SOLICITADAS CON FINES DE VENTA DIRECTA

La LGT dispone que los abonados a los servicios de comunicaciones electrónicas tengan el derecho a no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de venta directa sin haber prestado su consentimiento previo e informado para ello.

Por su parte, el Real Decreto 424/2005, distingue dos tipos de llamadas no solicitadas con esa finalidad:

1. Las llamadas no solicitadas por los abonados con fines de venta directa que se efectúen mediante sistemas de llamada automática, a través de servicios de comunicaciones electrónicas, sin intervención humana (aparatos de llamada automática) o facsímil (fax), sólo podrán realizarse a aquellos destinatarios que hayan dado su consentimiento previo, expreso e informado.

2. Las llamadas no solicitadas por los abonados con fines de venta directa, que se efectúen mediante sistemas distintos de los anteriores (principalmente, mediante la intervención de un operador) pueden efectuarse, salvo las dirigidas a aquellos que hayan manifestado su deseo expreso de no recibirlas.

Tampoco pueden realizarse estas llamadas, a no ser que se cuente con su consentimiento expreso, a personas que no figuren, porque así lo han querido, en las guías de comunicaciones electrónicas (guías telefónicas), o a las que, apareciendo en ellas, hayan indicado que sus datos no sean utilizados con fines publicitarios o comerciales.

Recomendaciones a usuarios sobre llamadas no solicitadas con fines comerciales:

La Agencia Española de Protección de Datos ha elaborado las siguientes Recomendaciones sobre llamadas telefónicas con fines comerciales y publicitarios:

- El ciudadano no debe recibir llamadas automáticas sin intervención humana con fines de venta directa, a menos que haya consentido previamente y de forma expresa en su recepción.

- Si las llamadas son realizadas por una compañía con la que el ciudadano mantiene una relación contractual, podrá comunicarle su oposición a recibir llamadas con fines comerciales.

- Para no recibir llamadas comerciales a través de una línea de telefonía fija podrá solicitar al operador que no se publiquen sus datos en guías telefónicas públicas o que tales datos sean marcados de tal forma que no puedan ser utilizados con fines comerciales.

- Para evitar las llamadas aleatorias, el ciudadano únicamente puede manifestar su negativa u oposición ante los promotores de las mismas o, cuando en el futuro se constituyan ficheros comunes de exclusión promocional, podrá suministrar sus datos (incluyendo el número de línea móvil), para que puedan ser contrastados por los promotores de las llamadas.

Recomendaciones a las compañías:

- Las compañías deben verificar que los destinatarios de las llamadas comerciales no automáticas no figuren en las guías o no hayan ejercitado su derecho a que, aunque aparezcan, no sean utilizados con fines de publicidad.

- La normativa sobre protección de datos es aplicable exclusivamente en aquellos supuestos en los que la llamada comercial se efectúa en circunstancias en que el destinatario podría haber sido identificable para el promotor de la llamada.

- Los operadores de telecomunicaciones pueden tratar, con fines de promoción comercial de servicios de comunicaciones electrónicas, los datos de tráfico de sus propios clientes, en la medida y durante el tiempo necesarios para la prestación de tales servicios o su promoción comercial, siempre y cuando el abonado haya dado su consentimiento informado.

- Las compañías deben adaptar sus cláusulas contractuales para facilitar al cliente el ejercicio del derecho a oponerse a que sus datos sean usados para actividades de publicidad y prospección comercial.

- Las compañías establecerán procedimientos sencillos para facilitar al cliente, a lo largo de toda la relación contractual, el ejercicio gratuito de su derecho de oposición a la utilización de sus datos con fines publicitarios. En todo caso, el ejercicio de estos derechos no podrá suponer un ingreso adicional para la compañía.

- Las compañías pueden realizar llamadas comerciales a los clientes de otras compañías del mismo grupo empresarial, sólo si el destinatario de la llamada hubiera otorgado previamente su consentimiento informado a éstas.

- Las compañías no pueden tratar los datos de sus ex—clientes para la realización de llamadas telefónicas con fines comerciales (a menos que dispongan de su consentimiento).

- Al margen de su condición de clientes, las compañías pueden conservar los datos imprescindibles para identificar a aquellas personas que manifiesten su negativa a recibir publicidad (en particular la ofrecida a través de llamadas telefónicas).

- Cuando el destinatario de la llamada comercial no solicitada sea una persona física, la verificación de que ésta no ha manifestado su deseo de no recibir este tipo de llamadas deberá realizarse, también, a través de medios alternativos a las guías de abonados, (en particular mediante los ficheros comunes de exclusión del envío de comunicaciones comerciales).

- Las compañías no podrán efectuar llamadas telefónicas comerciales no solicitadas con datos de personas recomendadas a personas identificadas o identificables cuyos datos hayan sido proporcionados por sus propios clientes sin que aquéllas hubieran otorgado su consentimiento.

- La realización de llamadas a personas seleccionadas de los ficheros específicos de marketing requiere que éstos hayan sido informados claramente y que su consentimiento se extienda a ese tipo concreto de actividades promocionales.

11.5 COMUNICACIONES COMERCIALES POR VIA ELECTRONICA

a) ¿QUE SE ENTIENDE POR COMUNICACION COMERCIAL ELECTRONICA?

Comunicación comercial es toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

No tienen la consideración de comunicación comercial:

- Los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como:

  - **El nombre de dominio**

  - **La dirección de correo electrónico**

- Las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca, cuando sean elaboradas por un tercero y sin contraprestación económica.

Por ejemplo, el envío de boletines de noticias o boletines informativos no tiene la consideración de comunicación comercial, a no ser que ofrezcan algún producto o servicio. Se trataría únicamente de la prestación de un servicio de información al que se han suscrito voluntariamente los usuarios, aunque sea gratuito.

b) REQUISITOS GENERALES DE LA PUBLICIDAD COMERCIAL

Para estar dentro de la legalidad, las comunicaciones comerciales realizadas por vía electrónica deberán cumplir los siguientes requisitos:

- ✓ Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y la persona física o jurídica en nombre de la cual se realizan también deberán ser claramente identificables.

- ✓ En el caso que dichas comunicaciones tengan lugar a través de correo electrónico u otro medio de comunicación electrónica, la reciente modificación del art. 20.1 de la LSSI, vigente desde abril de 2014, elimina la obligación de identificar los e-mails o sms con la palabra ~~PUBLICIDAD~~ O ~~PUBLI~~, aunque se mantiene la necesidad de que sean claramente identificables las personas, físicas o jurídicas, que las realicen.

Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

Se prohíbe el envío de comunicaciones comerciales por medios electrónicos en las que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación, así como aquéllas en las que se incite a los destinatarios a visitar páginas de Internet que contravengan lo dispuesto en el artículo 20 de la LSSI.

Cuando las comunicaciones comerciales se remitan por correo electrónico, se deberá incluir necesariamente una dirección de correo electrónico valida donde los destinatarios puedan ejercer su derecho a oponerse al tratamiento de sus datos, quedando prohibido en el envío de las comunicaciones comerciales que no incluyan dicha dirección.

El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

En todo caso el destinatario deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando se utilicen datos personales procedentes de fuentes accesibles al público para la realización de comunicaciones comerciales, se proporcionará al destinatario la información que señala la LOPD y se ofrecerá al destinatario la oportunidad de oponerse a su recepción.

12 FICHEROS DE EXCLUSION PARA EL ENVIO DE COMUNICACIONES COMERCIALES “LISTAS ROBINSON”

12.1 FICHEROS DE EXCLUSION

Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlos y adoptar las medidas necesarias que eviten el envío de publicidad.

En estos casos, los responsables deben adoptar medidas que permitan identificar a aquellos que hayan manifestado su negativa a recibir publicidad, como por ejemplo, a través de una señal o marca asociada a sus datos personales. De este modo, antes de realizar una acción comercial o publicitaria, la entidad debe consultar el fichero del que es responsable para excluir a las personas que hayan manifestado su negativa a recibir publicidad o hayan ejercido su derecho de oposición.

b) Listas Robinson

Las Listas Robinson son unos ficheros de exclusión creados con la finalidad de evitar la recepción de publicidad no deseada. Los “Robinsones” son los consumidores que han manifestado su voluntad de no recibir comunicaciones comerciales no solicitadas.

Las listas Robinson tienen por objeto:

- Permitir a los consumidores eliminar su nombre y dirección de los listados de publicidad con el fin de evitar la recepción de publicidad que reciben en forma de mailing.

- Permitir a aquellos consumidores que estén interesados en recibir más envíos publicitarios, y en particular, sobre algún tema determinado, formar parte de manera gratuita de lo que se conoce como “Lista de Preferencia”, recibiendo exclusivamente publicidad sobre aquellos servicios o productos previamente seleccionados.

La utilización de estas listas:

- Constituye una muestra de respeto al consumidor.

- Supone una ventaja para las empresas, que, empleándolas evitan gastos innecesarios y excluyen de sus campañas a las personas no predispuestas para recibir una oferta.

El RLOPD dispone que será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de:

- La existencia de los ficheros comunes de exclusiones generales o sectoriales.
- La identidad de su responsable y su domicilio.
- La finalidad del tratamiento.

El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

12.2 PASOS A SEGUIR PARA EL TRATAMIENTO

Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Esta obligación es aplicable tanto a quienes se dediquen de forma principal o profesional a la publicidad, como a quienes realicen acciones promocionales puntualmente.

Con fecha 30 de junio de 2009 se ha puesto en marcha el primer fichero de exclusión con el que los ciudadanos podrán gestionar la publicidad que reciben por teléfono (fijo o móvil), por correo electrónico o por correo postal.

La Federación de Comercio Electrónico y Marketing Directo (FECEMD) ha llegado a un importante acuerdo con la AEPD para la nueva regulación de la lista de exclusión publicitaria, denominada Lista Robinson.

La nueva Lista Robinson que, a partir de la entrada en vigor del nuevo Reglamento de la LOPD, es obligatoria para todas las empresas u otras entidades que hacen publicidad con datos obtenidos de fuentes accesibles al público o de terceros, se aplicará a correo postal, e-mail, teléfono y SMS o MMS.

FECEMD, como forma de mostrar el compromiso de las empresas y otras entidades con el derecho a la protección de datos de los ciudadanos, viene prestando este servicio únicamente para correo postal desde hace más de 12 años.

Se trata de un fichero de exclusión publicitaria en el que los interesados que se inscriban podrán seleccionar por sí mismos los medios a través de los cuales no quieren recibir publicidad (correo postal, teléfono, correo electrónico, SMS o MMS) de las entidades que, para el desarrollo de las campañas publicitarias, empleen datos personales obtenidos de fuentes públicas (como guías telefónicas) o bases de datos de las que no sean responsables. La inscripción será efectiva en el plazo de tres meses.

Los ciudadanos pueden acceder gratuitamente a esta herramienta a través de www.listarobinson.es, inscribirse y seleccionar el medio o medios a través de los que no quieren recibir publicidad.

El servicio sirve tanto para la publicidad que las compañías envían a usuarios con quienes no han tenido ninguna relación comercial y cuyos datos han sido extraídos de directorios públicos, como las guías telefónicas, como para aquellas que ofrecen sus productos o servicios a sus propios clientes.

Este servicio de consulta y exclusión que tenía carácter voluntario, desde la aprobación del RLOPD y de acuerdo con lo dispuesto en los artículos 48 y 49, ha adquirido carácter obligatorio.

Por ello, todas las empresas u otras entidades que realicen acciones publicitarias para cuyo desarrollo sea necesario el tratamiento de datos de carácter personal deben consultar el fichero de Lista Robinson y excluir de las campañas publicitarias que realicen a aquellas personas que figuren en el mismo, siempre y cuando, el origen de los datos que se trate sea de fuentes accesibles al público o de otros responsables de ficheros.

13 LA PROTECCION DE DATOS EN LAS RELACIONES LABORALES

13.1 NORMATIVA INTERNA DE PROTECCION DE DATOS Y RR.HH.

Conforme al art. 89 del RD 1720/2007 de 21 de Diciembre, todos los empleados de una empresa que tengan acceso a datos considerados de carácter confidencial deberán tener conocimiento de la NORMATIVA INTERNA DE PROTECCION DE DATOS, cuyos aspectos más importantes resaltamos a modo de ejemplo a continuación.

Carácter de información confidencial

Se entiende por Información Confidencial: La información de carácter económico, financiero, técnico, comercial, estratégico, administrativo, económico o de otro tipo, que, en cualquier momento durante la vigencia del contrato de trabajo sea conocida o creada por la empresa y/o persona trabajadora en el desempeño de sus funciones profesionales.

Confidencialidad de los empleados respecto a la información

La persona trabajadora se obliga a conservar y tratar con la máxima diligencia y confidencialidad toda la Información Confidencial y, en particular, a no revelar a ningún tercero, sin el consentimiento previo de la empresa. En especial, las personas trabajadoras que en el desempeño de sus funciones profesionales, accedan, usen y/o traten Información Confidencial, incluidos los datos personales registrados en ficheros de datos personales, quedan obligados al cumplimiento de las siguientes obligaciones:

a- La persona trabajadora sólo tratará y utilizará aquella Información Confidencial que sea necesaria para el desarrollo de las funciones profesionales propias del puesto que ocupa dentro de la estructura de la empresa.

b- La persona trabajadora queda obligado a seguir las instrucciones fijadas por la empresa en todo lo que respecta al tratamiento de los Información Confidencial, no pudiendo utilizar y/o tratar dicha información para fines distintos de los expresamente indicados.

c- La persona trabajadora queda obligado al cumplimiento del deber de secreto respecto de la Información Confidencial a la que tenga o haya tenido acceso durante o como consecuencia del desempeño de las funciones profesionales en la empresa teniendo dicho deber de secreto una duración indefinida, una vez extinguido el contrato que une a la persona trabajadora con la empresa.

d- La persona trabajadora queda obligado a tratar dicha Información confidencialmente, quedando expresamente prohibida cualquier tipo de comunicación, cesión, transferencia, almacenamiento, envío o entrega, no autorizadas expresamente, de cualquier Información Confidencial a la que tenga o haya tenido acceso en el desempeño de sus funciones profesionales, tanto en formato físico como en formato electrónico, ya sea a las personas trabajadoras de la misma empresa no autorizados para acceder a dichos datos, ya sea a terceros ajenos a la estructura organizativa de la empresa. Tampoco podrá grabar Información Confidencial en disquetes u otros soportes magnéticos, ni imprimirlos o extraerlos fuera de las dependencias físicas donde desarrolle sus funciones profesionales sin que exista justificación alguna.

e- La persona trabajadora adoptará las medidas necesarias para evitar que terceros no autorizados puedan acceder a Información Confidencial y a limitar el acceso a tales elementos a los empleados autorizados que precisen disponer de ella para la ejecución de su trabajo, trasladándoles idéntica obligación de confidencialidad.

f- Las personas trabajadoras deberán guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral con la empresa tanto en soporte material como electrónico. Esta obligación continuará vigente tras la extinción del contrato laboral.

g- Ninguna persona trabajadora deberá poseer, para usos no propios de su responsabilidad, ningún material o información propiedad de la empres tanto ahora como en el futuro.

El incumplimiento por parte de la persona trabajadora de cualesquiera de los términos, condiciones y obligaciones anteriormente descritos puede constituir un delito de revelación de secretos, previsto en el artículo 197 y siguientes del Código Penal y determinará la responsabilidad de aquel frente a todas las demandas, acciones y/o reclamaciones que contra la empresa puedan dirigirse o ejercitarse. Dicho incumplimiento será calificado como una falta muy grave, pudiendo sancionarse en consecuencia de conformidad con las normas legales de aplicación.

Protección de datos

Toda persona trabajadora que en desarrollo de su trabajo recabe datos de carácter personal de clientes, proveedores, otros empleados o terceros en general para su incorporación a un fichero automatizado o papel, deberá hacerlo acorde con las directrices dispuestas por el responsable de seguridad y por la Ley Orgánica de Protección de Datos a la que deberá ajustarse en todo caso.

Son actos prohibidos:

- Cruzar información relativa a datos de diferentes ficheros o servicios con el fin de establecer perfiles de personalidad, hábitos de consumo o cualquier otro tipo de preferencias, sin la autorización expresa del responsable de seguridad.

- Cualquier otra actividad expresamente prohibida en este documento o en las normas sobre protección de datos e Instrucciones de la Agencia de protección de Datos.

- Sacar soportes y ordenadores personales fuera de los locales de la organización sin autorización previa.

Medidas de seguridad

Queda prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si la persona trabajadora sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento del responsable del sistema, con el fin de que le asigne una nueva clave. Ante una baja o ausencia temporal del usuario, el responsable del

departamento podrá solicitar al responsable del sistema la cesión de clave o datos a la persona por él designada.
La persona trabajadora está obligado a utilizar la red corporativa y la intranet de la empresa y sus datos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de o de terceros, o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.

El usuario está obligado a introducir una contraseña. Se evitarán nombres comunes, numero de matriculas de vehículos, teléfonos, nombres de familiares, amigos, etc., y derivados del nombre de usuario como permutaciones o cambio de oren de las letras, transposiciones, repeticiones de un único carácter, etc.

Activar el salvapantalla para periodos de inactividad mayores de 10 minutos.

En el caso que sea necesario la duplicación de los documento, impresión de los mismos o traslado fuera de centro, la persona trabajadora está en la obligación de reflejar en un documento de Entrada/Salida los movimientos de los contenidos duplicados o documento originales; previa autorización del Responsable.

Todos los documentos que sean impresos y que contengan datos de carácter personal, su retirada de las bandejas de las impresoras o fotocopiadoras, es responsabilidad de la persona que realiza dichos procesos, la pérdida o extravíos de estos documento puede acarrear medidas de carácter disciplinarias o administrativas según correspondan.

Toda documentación a la que tenga acceso, que contenga datos de carácter personal y que no sea necesaria su conservación, está en la obligación de destruirla, de forma tal que imposibilite la obtención de dichos datos. Los documentos (folios) que contengan datos de carácter personal no pueden ser reutilizados, al menos, que se garantice su custodia y posterior destrucción una vez no sean necesarios.

Las mesas/despachos de las personas trabajadoras, que contengan carpetas o documentos con datos de carácter personal, deben tener los mecanismos de control necesarios que permitan su recogida, almacenamiento y custodio una vez que abandonen el puesto, o concluya su jornada laboral (archivadores con llave).

La persona trabajadora debe velar constantemente por la privacidad de los datos contenidos en los documentos, tomando las medidas necesarias para evitar que puedan ser leídos o vistos por persona ajena no autorizada, cumpliendo con el deber de secreto.

Los documentos en papel deben estar colocados de forma ordenada en lugares adecuados para su conservación, localización y acceso permitiendo garantizar de forma eficiente su localización con el objeto de cumplir los plazos en el ejercicio de los Derechos de los Afectados.

Los documentos que se encuentren en proceso de revisión, modificación o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentra a cargos de la misma deberán custodiarla e impedir en todo momento que pueda ser accedida por personas no autorizadas.

Registro de Incidencias

Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.

Las personas trabajadoras que tengan acceso a Información Confidencial para su actividad, están en la obligación de la custodia de los mismos, así como a informar a su responsable de las incidencias que puedan ocurrir durante su tratamiento.

Es obligación de todos las personas trabajadoras de la empresa comunicar al responsable del sistema cualquier incidencia que se produzca en los sistemas de información, así como en los archivos y documentos con datos de carácter personal a que tengan acceso.

Estarán prohibidas las siguientes conductas:

- Compartir o facilitar el identificador de usuario y la contraseña facilitada por la empresa con otra persona física o jurídica, incluido el personal de la propia institución.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la empresa.
- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario (Spam).
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la empresa y de terceros.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema.
- Introducir, descargar de Internet, reproducir, utilizar, instalar o distribuir programas informáticos no autorizados expresamente por la empresa cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- Borrar cualquiera de los programas instalados legalmente.
- Utilizar los recursos telemáticos de la empresa incluida la red Internet para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.
- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la empresa en su red corporativa.

13.2 EL CORREO ELECTRONICO E INTERNET COMO HERRAMIENTAS DE TRABAJO

El acceso a internet, el correo electrónico y la red corporativa o el teléfono son herramientas de trabajo que EHLABE. pone a disposición de sus empleados, por lo que su uso debe ser exclusivamente profesional.

Conductas no permitidas:

- ❖ Uso del correo corporativo, el acceso a internet o redes sociales, el uso del teléfono con fines personales y en horas de trabajo.
- ❖ Sacar información profesional sin el cumplimiento de las normas de seguridad o sin autorización
- ❖ Permitir acceso a la información a terceros no autorizados

13.3 USO DE TECNOLOGIAS DE CONTROL Y VIGILANCIA EN EL TRABAJO Y EL CONTROL DE ACCESO Y LOS CCTV

La empresa está facultada para adoptar una serie de medidas que hagan posible el control de la actividad laboral de sus empleados, de acuerdo con lo establecido en el Art. 20.3 y 4 Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de las personas trabajadoras:

¿Cuáles son las medias de control que puede Adoptar?

- ✓ Controles biométricos (huella digital, iris)
- ✓ Video vigilancia
- ✓ Controles sobre los ordenador:
  - ▪ Revisiones análisis o la motorización remota
  - ▪ Indexación de la navegación por internet
  - ▪ La revisión y motorización del correo electrónico y/o del uso de ordenadores
- ✓ Controles sobre la ubicación física de la persona trabajadora mediante la geolocalización

Nota: Es imprescindible cumplir con el deber de información a los empleados para que el control empresarial se realice en el marco de los principios de protección de datos.

Para que dicho control sobre la actividad laboral de los empleados no suponga una violación a la intimidad de las personas trabajadoras o cualquier otro derecho fundamental y se lleve a cabo conforme a la LOPD, la empresa deberá cumplir con el deber de informar y advertir a las personas trabajadoras de los siguientes extremos:

- De la posibilidad de que el uso de internet y el ordenador sean intervenidos
- De la existencia de las políticas internas o protocolos de la empresa para el uso de los sistemas informáticos.

13.4 EL ACCESO A LA INFORMACION POR EL COMITE DE EMPRESA Y LA PROTECCION DE DATOS

La Ley atribuye a los Delegados de Personal o al Comité de Empresa como órganos representativos del conjunto de personas trabajadoras al acceso a determinados datos de carácter personal de las personas trabajadoras, con la finalidad de cumplir con las funciones de vigilancia y control recogidas en el artículo 64.1.

En este sentido, el Comité deberá, en el ejerció de sus funciones, actuar dentro del marco de aplicación de la normativa de protección de datos y con sujeción a los siguientes principios:

- **Principio de calidad del dato**: Solo podrá tratar los datos a los que tiene acceso de conformidad con el artículo 64 .1 del ET, ya que en el caso de que los utilizase para cualquier otra finalidad distinta del correcto desenvolvimiento y control de la relación laboral vulneraría el principio de calidad del dato anteriormente analizado en el punto 5.1.

- **Medidas de seguridad**: el Comité de Empresa deberá adoptar las medidas de seguridad para garantizar la seguridad de los datos de carácter personal.

- **Deber de secreto**: los miembros del Comité de Empresa o Delegados de Personal quedarían obligados al deber de secreto y confidencialidad respecto de la información a la que tuvieran acceso en el transcurso del desarrollo de su actividad. Además dichas obligaciones subsistirían aun después de finalizar sus funciones.

Por último, la empresa podría hacer firmar a todos los miembros del Comité de Empresa o Delegados de Personal un Documento de Confidencialidad por el que se comprometerían de forma expresa y por escrito a cumplir con los principios de protección de datos anteriormente analizados.

13.5 SISTEMAS DE DENUNCIAS INTERNAS “WHISTLEBLOWING”

Los sistemas de denuncias internas o Whistleblowing, son considerados como una cuestión de buen gobierno corporativo dentro del ámbito de la empresa, a través del cual los empleados pueden poner de manifestó las conductas contrarias a la Ley o las normas de conducta internas de la empresa. Dichos sistemas, se suelen configurar, mediante la creación de buzones internos, generalmente mediante procedimientos online.

Pues bien, para que el establecimiento de dichos sistemas se realice de conformidad con la normativa de protección de datos vigente, es necesaria la observancia de los siguientes principios de protección de datos:

Principio de Proporcionalidad: La denuncias tienen que ir referidas única y exclusivamente a que los hechos o supuestas actuaciones de la persona trabajadora, tenga una efectiva implicación en la relación entre la empresa y su personal, y que se refirieran a una violación de las normas internas de la empresa como de las leyes, normativas o códigos éticos. Todo el personal de la empresa puede ser denunciante o denunciado en el sistema.

Deber de Información a las personas trabajadoras: Los empleados serán previamente informados de la existencia y finalidad del sistema de denuncias, su funcionamiento, la garantía de la confidencialidad de datos del denunciante y la garantía de la información al denunciado de la existencia de una denuncia.

Deber de Información al Denunciado: Se debe de informar al denunciado en el plazo más breve posible de los hechos denunciados y de los destinatarios de la información (el departamento responsable del sistema y de los derechos en materia de protección de datos).

Principio de Calidad del Dato: para garantizar la exactitud de la información deberán establecerse por parte de la empresa mecanismos que garanticen únicamente la aceptación de las denuncias en las que el denunciante aparezca claramente identificado, no siendo adecuado establecer un sistema de denuncias anónimas. El sistema incorporará los datos de denunciante y denunciado, los hechos denunciados y el resultado de las investigaciones.

Confidencialidad de la Identidad del Denunciante: La confidencialidad del denunciante deberá quedar a la salvo, no facilitándose como regla general, su identificación al denunciado.

Cesión de Datos: Si los datos contendidos en el sistema de denuncias fueran a ser trasmitidos una tercera empresa para que investigue el hecho tanto el denunciante como el denunciado deberán ser previamente informados de esta circunstancia.

Implementación de las Medidas de Seguridad: establecerse en relación a los tratamientos de datos las medias que garanticen la adecuada seguridad y confidencialidad de la información, pudiendo establecerse medidas reforzadas de seguridad y extremando las cautelas que garanticen el cumplimiento del deber de secreto.

Como regla general, la relación de medias que se pueden adoptar en los sistemas de denuncias internas son:

- Limitar el acceso al contenido de las denuncias a los usuarios que llevan a cabo la investigación y relacionarlos en el documento de seguridad
- Establecer un sistema de registro de accesos, aún cuando no corresponda aplicar las medidas de NIVEL ALTO
- Firmas de compromisos reforzados de confidencialidad con las personas que van a tener acceso autorizado a este sistema
- Medidas disuasorias para el caso que se vulnere el deber de secreto

Cancelación del Datos: Los datos serán cancelados cuando dejen de ser necesarios y tras el fin de las investigaciones si los hechos no hubiesen sido probados. En caso contrario, los datos ser conservaran el tiempo que sea necesario para el ejercicio de acciones que le pudieran corresponder a la compañía

Derechos Arco del Denunciado: En estos sistemas deberán garantizarse, los derechos de acceso, rectificación, cancelación y oposición por parte del denunciado, sin que ello implique facilitar el acceso a la identidad del denunciante.

13.6 PROCESO DE SELECCION Y CUSTODIA DE CV

Los primeros procesos de tratamientos de datos personales tienen lugar cuando la futura persona trabajadora es un simple candidato a un puesto de trabajo, en dicho caso el departamento de Recursos Humanos de la empresa deberá adoptar las siguientes medidas:

- Disponer de impresos de modelos tipo para la formalización del Currículum Vitae (CV) y de un procedimiento de formalización y entrega de los mismos por los candidatos, ya que ello permite no sólo informar adecuadamente sobre la finalidad y uso de los datos sino definir con precisión el tipo de datos a tratar, establecer las medidas de seguridad e informar de los procedimientos en el ejercicio de sus derechos.

- En caso de que la selección se realice a través de algún tipo de Anuncio o convocatoria pública debería incluirse en ella la información prevista en el artículo 5 de la LOPD.

- Dado el caso de que el CV sea presentado directamente por el candidato (sin previa solicitud de la empresa) deben establecerse procedimientos de información que supongan algún acuse o confirmación de conocer las condiciones en las que se desarrollará el tratamiento de los datos de carácter personal de los candidatos, por Ejemplo:

    - El CV se remitió por candidato a través de correo postal o electrónico y se cuenta con una dirección electrónica facilitada por el propio interesado, podemos remitirle la información por ese medio solicitando confirmación de la recepción y condicionando el tratamiento de los datos al acuse de recibo por parte del candidato o el interesado.

    - El CV se presentó por el candidato en un mostrador u oficina de atención, éste debería ser informado por cualquier medio que acredite el cumplimiento de este deber como por ejemplo carteles, documentos de acuse de recibo y en general cualquier medio que garantice y permita probar el cumplimiento del deber de información.

- En casos de grupos de empresas o de cualquier otra fórmula de colaboración empresarial debe tenerse en cuenta que la cesión de los datos contenidos en el CV o del propio documento debe contar con el consentimiento del candidato.

- Candidatos no seleccionados: para aquellos candidatos no seleccionados pero cuyo CV interese a la empresa conservar para futuras acciones, la empresa deberá informar al candidato de esta circunstancia dándole la posibilidad de ejercitar sus derechos ARCO.

- Conservación del CV: Durante el plazo de un año como máximo, después de dicho plazo, se deberá proceder a su destrucción en cumplimiento del principio de calidad del dato.

14 LA AGENCIA ESPAÑOLA DE PROTECCION DE DATOS

La Agencia Española de Protección de Datos es un ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada. Actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Sus funciones son:

- ✓ General
  - ➢ Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- ✓ En relación con los afectados
  - ➢ Atender a sus peticiones y reclamaciones
  - ➢ Información de los derechos reconocidos en la Ley
  - ➢ Promover campañas de difusión a través de los medios
- ✓ En relación con quienes tratan datos
  - ➢ Emitir autorizaciones previstas en la Ley
  - ➢ Requerir medidas de corrección
  - ➢ Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos
  - ➢ Ejercer la potestad sancionadora
  - ➢ Recabar ayuda e información que precise
  - ➢ Autorizar las transferencias internacionales de datos
- ✓ En la elaboración de normas
  - ➢ Informar los Proyectos de normas de desarrollo de la LOPD
  - ➢ Informar los Proyectos de normas que incidan en materias de protección de datos
  - ➢ Dictar Instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD
  - ➢ Dictar recomendaciones en materia de seguridad y control de acceso a los ficheros

- ✓ En materia de telecomunicaciones

    - ➢ Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente

- ✓ Otras funciones

    - ➢ Velar por la publicidad en los tratamientos, publicando anualmente una lista de los mismos (CD)

    - ➢ Cooperación Internacional

    - ➢ Representación de España en los foros internacionales en la materia

    - ➢ Control y observancia de lo dispuesto en la Ley reguladora de la Función Estadística Pública

    - ➢ Elaboración de una Memoria Anual, presentada por conducto del Ministro de Justicia a las Cortes

15 GLOSARIO DE TERMINOS (A-Z)

- **AEPD**: Agencia Española de Protección de Datos.
- **Accesos autorizados**: autorizaciones concedidas a un usuario para la utilización de los diversos recursos.
- **Afectado o interesado**: Persona física titular de los datos que sean objeto del tratamiento.
- **Autenticación**: procedimiento de comprobación de la identidad de un usuario.
- **Bloqueo de datos**: la identificación y reserva de datos para impedir su tratamiento.
- **Cesión o comunicación de datos**: Toda revelación de datos realizada a una persona distinta del interesado.
- **Consentimiento del interesado**: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- **Contraseña:** información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.
- **Control de acceso**: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
- **Copia del respaldo**: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
- **Datos de carácter personal**: Cualquier información concerniente a personas físicas identificadas o identificables.
- **Encargado del Tratamiento**: 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.
- **Fichero**: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- **Fuentes accesibles al público**: Aquellos ficheros 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, *exclusivamente,* el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

- **Identificación**: procedimiento de reconocimiento de la identidad de un usuario.

- **Incidencia**: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

- **LOPD:** Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

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

- **RGPD:** Registro General de Protección de Datos, perteneciente a la Agencia Española de Protección de Datos, en donde se registran los ficheros inscritos.

- **RDLOPD**: Real Decreto 1720/2007 de 21 de Diciembre, por el que se aprueba el nuevo Reglamento de Medidas de Seguridad

- **Recurso**: cualquier parte componente de un sistema de información.

- **Responsable de Seguridad**: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

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

- **Sistemas de información**: conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

- **Soporte**: objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

- **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.

- **Usuario**: sujeto o proceso autorizado para acceder a datos o recursos.